

**UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF TEXAS
DALLAS DIVISION**

MONEYGRAM PAYMENT SYSTEMS,
INC.,

Plaintiff,

v.

CAPGEMINI AMERICA, INC.,

Defendant.

§
§
§
§
§
§
§
§
§
§

Civil Action No. 3:25-cv-000498-S

**APPENDIX IN SUPPORT OF CAPGEMINI'S MOTION TO DISMISS PLAINTIFF
MONEYGRAM PAYMENT SYSTEMS, INC.'S AMENDED COMPLAINT**

In accordance with the United States District Court Northern District of Texas Local Rule 7.1(i), Defendant Capgemini America, Inc. submits the following Appendix in support of Capgemini's Motion to Dismiss Plaintiff MoneyGram Payment Systems, Inc.'s Amended Complaint:

TAB	DESCRIPTION	APP.
A	Declaration of Jack G. Tubio	App. 1-2
A-1	Business Services Master Agreement between MoneyGram Payment Systems, Inc. and Capgemini America, Inc.	App. 3-49
A-2	Statement of Work between MoneyGram Payment Systems, Inc. and Capgemini America, Inc.	App. 50-71
A-3	Document preservation letter from C. Feinberg on behalf of MoneyGram International, Inc. to Capgemini America, Inc., dated October 3, 2024	App. 72-74
A-4	Letter from T. Zalinski on behalf of Capgemini America Inc. to C. Feinberg, dated October 31, 2024	App. 75-77
A-5	Letter from S. Drake on behalf of MoneyGram International, Inc. to Capgemini America, Inc., dated November 27, 2024	App. 78-80

DATED: July 10, 2025

Jenny H. Kim (*pro hac vice*)
Jack G. Tubio (*pro hac vice*)
BOIES SCHILLER FLEXNER LLP
55 Hudson Yards
New York, New York 10001
Telephone: (212) 446-2354
Email: jkim@bsflp.com
jtubio@bsflp.com

Respectfully submitted,

/s/ Jeffrey M. Tillotson
Jeffrey M. Tillotson
State Bar No. 20039200
J. Austen Irrobali
State Bar No. 24092564
TILLOTSON JOHNSON & PATTON
1201 Main Street, Suite 1300
Dallas, Texas 75202
Telephone: (214) 382-3041
Facsimile: (214) 292-6564
Email: jtillotson@tillotsonlaw.com
airrobali@tillotsonlaw.com

Counsel for Defendant Capgemini America, Inc.

CERTIFICATE OF SERVICE

The undersigned hereby certifies that a copy of this document was forwarded to all counsel of record through the Court's CM/ECF System on July 10, 2025.

/s/ Jeffrey M. Tillotson
Jeffrey M. Tillotson

**IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF TEXAS
DALLAS DIVISION**



MONEYGRAM PAYMENT SYSTEMS,
INC.,

Plaintiff,

v.

CAPGEMINI AMERICA, INC.,

Defendant.

§
§
§
§
§
§
§
§
§
§
§

Civil Action No.
3:25-cv-00498-S

DECLARATION OF JACK G. TUBIO

Pursuant to 28 U.S.C. § 1746, I, Jack G. Tubio, declare under penalty of perjury as follows:

1. I am an attorney admitted to practice in New York and an associate at the law firm Boies Schiller Flexner LLP. I serve as counsel for Defendant Capgemini America, Inc. ("Capgemini") in this matter and am admitted Pro Hac Vice before this Court. (ECF 13)

2. I submit this declaration in support of Capgemini's Motion to Dismiss Plaintiff MoneyGram Payment Systems, Inc.'s Amended Complaint. As counsel for Capgemini, I am familiar with the information set forth in this declaration from personal knowledge and documents I have reviewed, including the documents annexed to this declaration.

3. Attached as **Exhibit A-1** is a true and correct copy of the Business Services Master Agreement, dated August 20, 2020, between MoneyGram Payment Systems, Inc. and Capgemini America, Inc.

4. Attached as **Exhibit A-2** is a true and correct copy of the Statement of Work, dated September 3, 2023, between MoneyGram Payment Systems, Inc. and Capgemini America, Inc.

5. Attached as **Exhibit A-3** is a true and correct copy of the document preservation letter, dated October 3, 2024, from Cory J. Feinberg, Esq. on behalf of MoneyGram International, Inc. to Capgemini America, Inc.

6. Attached as **Exhibit A-4** is a true and correct copy of the letter, dated October 31, 2024, from Traci Zalinski on behalf of Capgemini America, Inc. to Cory J. Feinberg, Esq.

7. Attached as **Exhibit A-5** is a true and correct copy of the letter, dated November 27, 2024, from Scott Drake on behalf of MoneyGram International, Inc. to Capgemini America, Inc.

I declare under penalty of perjury that the foregoing is true and correct. Executed in New York, New York on July 10, 2025.

/s/ Jack G. Tubio

Jack G. Tubio

EXHIBIT A-1

BUSINESS SERVICES MASTER AGREEMENT

This Business Services Master Agreement (this “**Agreement**”) is made and entered into effective August 20, 2020 (the “**Effective Date**”) by and between MoneyGram Payment Systems, Inc., with offices located at 1550 Utica Avenue South, St. Louis Park, MN 55416 (“**MPSI**”) and Capgemini America, Inc., with its principal offices located at 79 Fifth Avenue, 3rd Floor, New York, NY 10003 (“**Supplier**”). Supplier and Customer are jointly referred to as the “**Party**” or “**Parties**,” as applicable.

RECITALS

Supplier is a provider of certain business services. Such services are being requested by MPSI and any entity controlling, controlled by or under common control with MPSI (“**Affiliates**”) (collectively “**Customer**”).

Customer and Supplier desire that Supplier provide certain services to Customer as more fully described in a statement of work (“**SOW**”) executed pursuant to this Agreement, all of which will be subject to the terms and conditions of this Agreement.

AGREEMENT

In consideration of the promises and mutual covenants set forth in this Agreement, and for other good and valuable consideration, the receipt and sufficiency of which are hereby acknowledged, the Parties hereby agree as follows:

1. **Services.**

- 1.1. **Business Services.** During the Term of this Agreement, as defined in Section 9.1 below, Supplier agrees to render services to Customer, as authorized by Customer from time to time at Customer’s discretion (the “**Services**”). Customer has implemented a centralized vendor management solution (“**VMS**”), owned and hosted by a third party (“**VMS Provider**”), which Customer will use to acquire, process and manage its Service needs. Prior to providing any Services, Supplier shall complete the VMS Provider’s registration process resulting in a registration link (“**VMS Registration**”). As part of the VMS Registration and to enable and authorize Supplier’s use of the VMS, Supplier will be required to agree to the VMS Provider’s end user license agreement or other similar agreements required by the VMS Provider to allow Supplier to access and utilize the VMS (collectively, the “**VMS Provider Agreements**”). Supplier may provide Services to Customer only upon successful completion of the VMS Registration and execution of any VMS Provider Agreements. All Services will be authorized and agreed to by Customer through Customer’s approval in the VMS of Assignments, Projects, Bids, SOW or other mechanisms described and defined in the VMS and/or the VMS Provider Agreements (in each case a “**VMS Authorization**”). For Services requiring a detailed requirements definition, schedule and/or the creation and delivery of Deliverables (as defined herein below) (“**Project Services**”), the execution of an SOW as described in this Agreement will be required in addition to the VMS Authorization. In the event Services are purchased through a VMS Authorization only, and no SOW is executed, the VMS Authorization shall be deemed an SOW governed under the terms of this Agreement. Supplier shall not be authorized to render any Services until a valid VMS Authorization has been issued in accordance with this Agreement and, if Project Services will be delivered, an SOW has been signed by an authorized representative of Customer for such Services.



- 1.2. **Statements of Work.** Each SOW shall incorporate and be governed by all of the terms and provisions of this Agreement. The terms and provisions of each SOW shall be considered a part of this Agreement. Unless otherwise expressly provided in this Agreement or in an SOW, if any term or provision contained in an SOW conflicts with any term or provision of this Agreement, the terms or provisions of this Agreement shall govern. A sample form SOW is attached hereto as **Exhibit A**, but Customer and Supplier may agree upon a different format as long as the SOW includes, without limitation, the terms that are required in sections (a) through (j) below:

- (a) **Specification.** Each SOW shall contain a detailed specification, which shall include a description of the Services and a description of the Deliverables, if any, as mutually agreed upon between Customer and Supplier (the “**Specification**”).

Customer may elect at any time and from time to time to modify the Specification, by notice thereof to Supplier. Such notice should indicate whether Customer is requesting a reduction in the fee or a new estimate because the scope of the Specification has narrowed. If Supplier objects to any proposed Specification modification or if such modification will change the agreed upon fee or impact the estimate, Supplier shall notify Customer of its objections, or any proposed changes to the fee or estimate in detail and in writing within ten (10) business days after receiving the proposed modification to the Specification. On a good faith basis, Supplier and Customer will attempt to resolve any objections to a proposed modification to the Specification consistent with Customer’s overall requirements and negotiate any change in the fee or estimate.

- (b) **Schedule.** Each SOW shall contain a schedule for the delivery of the Services and/or the Deliverables (the “**Schedule**”). Each VMS Authorization will set forth the start and end date for the Services. Any extension of the end date set forth in a VMS Authorization will require Customer to approve a new VMS Authorization covering the extended period for the Services. Customer shall not be obligated to pay for any Services delivered by Supplier which are delivered beyond the stated end date set forth on the VMS Authorization.

Personnel. The individuals provided by Supplier to perform the Services under the Agreement shall be referred to hereinafter as the “Personnel.” With respect to each of Supplier’s Personnel delivering Services to Customer, the Supplier shall provide Customer any information Customer may reasonably request regarding the Personnel, which may include but is not limited to: (1) full legal name of Personnel (including legal first name, middle name and surname); (2) preferred name; (3) birth month and birth day of Supplier Personnel; (4) the title and/or skill level of the Personnel; (5) confirmation of prescreening measures for each of Supplier’s Personnel as set forth in Section 1.6 below; (6) if Supplier has engaged a subcontractor to deliver the Services as set forth in Section 1.5, Supplier will provide the name of the entity or firm that Supplier is engaging as a subcontractor (7) whether the Personnel are W2 or 1099; and (7) visa type, visa status, and expiration date of the visa for each Supplier Personnel, if applicable.

- (c) **Assistance by Customer.** Each SOW shall describe the assistance, equipment or software, if any, which Supplier will require from Customer. Customer shall not

be required to allow Supplier access to Customer's facilities after normal business hours unless otherwise specified in the applicable SOW.

- (d) **Fees, Materials and Expenses.** Each SOW shall specify whether the delivery of the Services is on a fixed fee or a "not to exceed" time and materials basis and state the amount of the fixed fee or the time and materials estimate. The fixed fee or not to exceed time and materials estimate set forth on the VMS Authorization shall not be exceeded without Customer's approval of a new VMS Authorization covering any excess amount. Customer shall not be obligated to pay for any Services delivered by Supplier which are in excess of the fixed fee or time and materials estimate set forth on the VMS Authorization.

- i. **Time and Materials Estimate.** If the Services are to be delivered on a time and materials basis, the SOW shall contain a detailed estimate of all of the time, materials and expenses, including travel expenses, to be rendered under that SOW (the "**Estimate**") and also identify any limitations, dependencies or assumptions that were relied upon in arriving at the Estimate that might impact the Estimate.

Unless authorized in advance and in writing by Customer, charges invoiced under a SOW will not exceed such Estimate. If at any time Supplier reasonably believes, knows, or anticipates that the expected amounts to be invoiced to Customer under a SOW might exceed the applicable Estimate, Supplier will immediately notify Customer of the anticipated cost increase and indicate the reasons for such increase in which case Customer, in its sole discretion, may elect to: (i) terminate the SOW pursuant to Section 8.2; (ii) continue the SOW under the agreed upon terms and conditions; or (iii) negotiate revised terms and conditions for the completion or continuation of said SOW. If Customer elects to negotiate revised terms and conditions for the completion or continuation of said SOW, Supplier shall negotiate in good faith and make all reasonable efforts to continue or complete the SOW at the lowest cost possible.

- ii. **Fixed Fee.** If the Services are to be delivered on a fixed fee basis, the SOW shall include a description of any materials to be provided, whether travel or other expenses are included and identify any limitations, dependencies or assumptions that were relied upon in determining at the fee. If travel or other expenses are not a component of the Fixed Fee, a detailed estimate of such expenses shall be included.

- (e) **Travel and Incidental Expenses.** Unless separately specified, estimated and agreed to in the applicable SOW, all fees payable under any SOW shall include all incidental and travel expenses. In the event travel and other incidental expenses are separately specified and agreed to in the applicable SOW, Customer will be responsible for payment of actual, reasonable and customary expenses for travel, lodging and meals provided such expenses have been pre-approved by Customer, are submitted in the VMS with appropriate documentation and have been included in the time and materials estimate or are estimated as a separate component of a fixed fee.

- (f) **Deliverables.** If applicable, each SOW shall specify the development materials, reports or other tangible outputs resulting from the delivery of the Services

(collectively the “**Deliverable(s)**”) to be provided, developed and/or delivered by Supplier to Customer in accordance with the Schedule for that SOW.

- (g) **Key Persons.** The Parties agree that there may be certain of Supplier’s Personnel who are essential to the accomplishment of the Services set forth in this Agreement or a particular SOW (“**Key Persons**”). Each SOW shall specifically identify any Key Persons.

If at any time during the performance of such SOW these Key Persons are no longer active on Customer’s account or employed by Supplier for whatever reason, Supplier shall immediately notify Customer and Customer shall have the right to terminate the SOW immediately upon written notice to Supplier. If Customer gives notice of such termination to Supplier, Supplier shall immediately cease the work under the applicable SOW.

- 1.3. **Right to Audit.** Customer will have the right during the term of this Agreement and for twenty-four (24) months after termination of the Agreement or any SOW, to audit the books, records and operations of Supplier insofar as may be necessary to determine Supplier’s compliance with its obligations under this Agreement. Unless mutually otherwise agreed to by the parties, audits will be limited to one time per year and will be performed at the expense of the Customer. Customer and Customer’s independent auditors will have access to Supplier’s books, records and operations at all reasonable times, with prior written notice and Supplier agrees to cooperate to reasonable requests to enable Customer and its independent auditors to carry out the intent and purposes of this section. Customer may notify Supplier of any deficiencies in performance discovered in any such audit, which deficiencies shall be promptly corrected by Supplier. In the event an audit discloses any billing discrepancy in Customer’s favor, Supplier shall, at Customer’s option, refund the amount of any such overpayment within thirty (30) days after receipt of written notice from Customer or credit the amount of such overpayment to subsequent invoice(s).
- 1.4. **Subcontractors.** Supplier may not use subcontractors to perform the services unless such subcontractors are first approved by Customer. Customer’s approval of any subcontractor must be agreed to by Customer in a writing signed by an authorized representative of MoneyGram. If use of a subcontractor is authorized by Customer in accordance with this Section 1.5, then (i) the use of the authorized subcontractors by Supplier is at Supplier’s sole expense; and (ii) prior to engaging any authorized subcontractor to perform Services for Customer, Supplier shall provide Customer with the bill rate Supplier will pay for any subcontractor resource and/or other information related to the amount Supplier will pay to the subcontractor for the performance of the subcontracted portion of the Services. Customer shall have the sole right to reject any of Supplier’s subcontractors whose qualifications, in Customer’s sole judgment, are insufficient for the satisfactory performance of the obligations required by this Agreement or for any other reason. Where subcontractors are used, Supplier shall remain responsible for the performance of Services by any subcontractor, and all subcontractors employed by Supplier shall be subject to all provisions of this Agreement. Any subcontractors shall be identified as such on the applicable SOW once they have been accepted by Customer.
- 1.5. **Pre-screening of Personnel.** Supplier shall conduct the following screening measures for the specified Personnel: OFAC screening in compliance with the warranty set forth 10.11 below, verification of previous employment, seven panel drug testing utilizing the protocol attached hereto as **Exhibit B** and criminal background checks. The screening measures

are to be conducted at Supplier's expense. Further, Supplier is responsible for complying with all federal, state and municipal laws and regulations applicable to these screening measures. Subject to such laws and regulations, Supplier agrees to comply with the following:

- (i) At a minimum, the criminal background check must include a lifetime all-US felony background check and a misdemeanor check in the county or counties in which the individual has resided and worked within the previous seven (7) years. The Personnel may begin work under this Agreement only if there are no convictions other than for minor traffic offenses or if the Customer's Human Resources Department approves the assignment. At no time can anyone with a felony conviction work for Customer in any capacity.
- (ii) At Customer's request, Supplier agrees to provide Customer with certification that the above-mentioned screening was conducted on its Personnel in compliance with this paragraph in the form attached hereto as **Exhibit F**.

- 1.6. **Background Checks.** Supplier Personnel assigned to perform Services under this Agreement shall have undergone industry standard background verification which include Social Security Number; Credit History; Criminal History; Employment; Education; and Global Sanctions checks.
- 1.7. **Acceptance of Deliverables.** For each respective SOW, Supplier will deliver the applicable Deliverables, if any, to Customer pursuant to the Schedule contained in that SOW. Unless otherwise stated in the applicable SOW, promptly after receipt of a Deliverable, but no more than 5 business days, Customer will notify Supplier in writing of Customer's acceptance ("**Acceptance**" or "**Accepted**") or rejection of the Deliverable. If Customer does not expressly accept or reject Deliverables within 5 business days the deliverables will be deemed accepted. If Customer rejects the Deliverables, Supplier will, at its sole expense, promptly make all changes or modifications necessary for the Deliverable to comply with the Specifications, but in no event more than thirty (30) days after notice of rejection from Customer. If Deliverables have not been Accepted by Customer at the end of thirty (30) days because of Supplier's continued noncompliance with the applicable Specifications, Customer shall have no responsibility for payment to Supplier under the SOW for the nonconforming Deliverables.
- 1.8. **Discretion.** Supplier will exercise its own reasonable discretion in determining how Supplier performs the Services, subject to the terms of this Agreement. Notwithstanding anything contrary in the Agreement, Supplier may perform the Services with personnel of Supplier or any of its affiliates (each, a "Supplier Entity" and, collectively, "Supplier Entities") or with subcontractors of Supplier Entities without obtaining prior consent. Supplier shall be solely responsible for the performance of the Services and all of the other liabilities and obligations of Supplier under this Agreement, whether or not performed, in whole or part, by Supplier, any other Supplier Entity, or any subcontractor of any Supplier Entity. Customer shall have no recourse against, and shall bring no claim against, any other Supplier Entity or any subcontractor of any Supplier Entity or any member, shareholder, director, officer, manager or employee of any Supplier Entity or any subcontractor of any Supplier Entity with respect to any liability or obligations herein or in connection with the Services.

2. Fee Submission and Payment.

- 2.1 **Service Fee Submission through VMS.** To receive payment, as may be specified and required by the VMS, Supplier shall submit an itemized and detailed Timesheet, Expense, Milestone / Deliverable, and/or Miscellaneous Fees (if applicable) including but not limited to Sales Tax. Such submissions shall be completed weekly, monthly, upon completion, or as otherwise agreed by the Parties, or as may be specified by the VMS. Upon review of submissions by Supplier and verification/approval by the appropriate Customer representative, Customer may approve each submission. If the submission is approved by Customer, the VMS will generate an invoice for Services, including any reimbursable Expense and/or Taxes ("**Invoice**"). Such Invoice will then be routed to Customer's Accounts Payable Department for disbursement of payment pursuant Section 2.2 of the Agreement ("**Invoice Date**").
- i. With the exception of Miscellaneous Fees, Expenses, and Sales Taxes (if applicable), a two percent (2%) service fee shall be deducted from each Invoice ("**Supplier Fee**"). Supplier shall not increase their fees to offset and/or change the Supplier Fee.
 - ii. Supplier Personnel shall not be authorized for overtime without prior approval by the appropriate Customer representative.
 - iii. Each Invoice shall reference the Invoice Number, Assignment Number, and/or Project Number.
 - iv. All Invoices must be generated electronically through VMS.
 - v. SUPPLIER UNDERSTANDS THAT ANY SERVICES PROVIDED TO THE CUSTOMER WITHOUT A VMS AUTHORIZATION ARE DONE SO AT SUPPLIER'S OWN RISK, AND CUSTOMER WILL NOT BE LIABLE TO SUPPLIER FOR PAYMENT IN CONNECTION WITH ANY SERVICES PERFORMED OUTSIDE THE VMS PROCESS.
- 2.2 **Payment.** Invoices shall be paid net sixty (60) days from Invoice Date. Customer may, at its sole discretion, take a two percent (2%) discount if payment is sent within ten (10) days Invoice Date (Invoices processed as 2% 10 net 60).
- 2.3 **Set-Off.** Without prejudice to any other right or remedy it may have, upon mutual agreement of the parties Customer may set off amounts owing to it by Supplier resulting from a specific SOW against any amount payable by Customer to Supplier under that specific SOW.
- 2.4 **Taxes.** Supplier shall pay all taxes that are: (i) lawfully imposed by any governmental authority; (ii) on, based on, or measured by, gross or net income or gross or net receipts (including any capital gains taxes or minimum taxes) of Supplier, or taxes which are capital, doing business, excess profits, net worth, or franchise taxes of Supplier; (iii) caused by or arising out of the willful misconduct or negligence of Supplier; or (iv) any interest, additions to tax, or penalties associates with the taxes set forth in (i), (ii), or (iii) above. Supplier shall in good faith and using best efforts supply Customer with such information and documents reasonably requested by Customer as are necessary or advisable for

Customer to (a) recover or seek a refund of any sales or use tax paid by Customer as a result of this Agreement; or (b) control or participate in any proceeding to the extent permitted herein.

3. **Ownership.**

Upon full payment, Supplier hereby assigns to Customer any and all rights, title and interest, including, without limitation, copyrights, trade secrets and proprietary rights, to the materials created by Supplier specifically for Customer hereunder and required to be delivered to Customer by virtue of their description or specification as a Deliverable in an applicable SOW. The Deliverables exclude all third party works and products whether or not included or embedded in the Deliverables. The Deliverables shall be deemed to be “works made for hire” under the federal copyright laws. Supplier agrees to give Customer reasonable assistance, at Customer’s expense, to perfect such assignment of such rights, title and interest. However, the Deliverables may contain tools, methodologies, techniques, models, designs, utilities, development objects, programs, program listings, systems, modules, analysis frameworks, leading practices, specifications, solutions, solution platforms, templates, frameworks, and dashboards owned or developed by Supplier prior to, independently from, or in the course of its engagement hereunder (and any modifications or enhancements thereto) (collectively, “Supplier Technical Elements”) and Capgemini retains exclusive ownership rights to all Supplier Technical Elements. Accordingly, to the extent that any such Supplier Technical Elements are integrated into any Deliverables, Supplier hereby grants to Customer a perpetual, worldwide, non-exclusive, paid-up, limited license to use, copy and modify such Supplier Technical Elements as integrated into such Deliverables for internal purposes only. Notwithstanding anything to the contrary in this Section, where Supplier utilizes as a subcontractor a third party software vendor to provide Services with respect to software under license to Customer from such subcontractor, Customer’s rights to any materials developed by such subcontractor, to the extent they would constitute a Deliverable if developed by Supplier, shall be subject to the terms of the software license agreement between Customer and such subcontractor. Notwithstanding anything to the contrary contained herein, Supplier retains all rights to its knowledge, experience and know-how (including processes, ideas, concepts and techniques) acquired in the course of performing the Services.

4. **Confidentiality.**

4.1 **Confidential Information.** In connection with the performance of the Agreement, the Parties have furnished or may in the future furnish to the other certain proprietary, non-public, confidential trade secret, and other such information. The term “Confidential Information” as used in this Section, includes all such information of the parties, their predecessors-in-interest, or their affiliates, now in existence or hereafter created. Confidential Information includes the following:

- (a) All customer-related information of the Customer, including but not limited to, account numbers, account balances, and personally identifiable data;
- (b) All personally identifiable data of Customer’s agents or business partners, including but not limited to, account numbers, account balances and financial information;
- (c) All information marked as “confidential” or with similar designation or otherwise treated as confidential and that which would be reasonably understood to be confidential;

- (d) All information protected by rights embodied in copyrights, whether registered or unregistered, or pending unpublished patent applications, “know how,” trade secrets, and any other intellectual property rights of the Parties;
- (e) All proprietary business, financial or technical information of the Parties or their affiliates and any of their respective customers, agents, business partners or vendors (including, but not limited to, customer lists, customer financial information and software licensed from third parties or owned by the Parties or their affiliates); and
- (f) Each Party’s marketing philosophy and objectives, promotions, markets, customer information, materials, financial results, technological developments and other similar confidential and or proprietary information and materials.

4.2 **Exclusions to Confidential Information.** Notwithstanding the foregoing, and except to the extent protected by copyright, patent, or trademark law and with the exception of Confidential Information described in Section 4.1 (a) and (b) above, Confidential Information shall not include any portion of such information which the other Party can establish by clear and convincing evidence to have:

- (a) become publicly known without breach of the Agreement; or
- (b) been known by the other Party without any obligation of confidentiality, prior to disclosure of such Confidential Information to the other Party; or
- (c) been received in good faith by the other Party from a third-party source having the right to disclose such information.

4.3 **Limited Use of Confidential Information.** The Parties may use the Confidential Information only for the purpose of performance of their obligations under this Agreement. Unless otherwise agreed to in writing between Customer and Supplier, from and after the date of the Agreement, the Parties shall:

- (a) not reproduce, copy, duplicate, divulge or use any Confidential Information, or allow any Confidential Information to be reproduced, copied, duplicated, divulged or used, except as expressly permitted herein;
- (b) require that all persons, employees, agents, partners, consultants, contractors, representatives of the Parties, and any other third parties (collectively, the “Representatives”) who are permitted access to any Confidential Information to agree to assume all of the same obligations regarding the protection of the Confidential Information assumed by the Parties under the Agreement;
- (c) keep all Confidential Information in a physically secure place which will prevent anyone, except the Representatives who are permitted access to the Confidential Information to satisfy the purposes of the Agreement, from using or disclosing any Confidential Information; and
- (d) if required by a court or governmental agency having proper jurisdiction to disclose any Confidential Information, the recipient of such request or order shall

promptly notify the owner of such Confidential Information of such request and/or order so that the owner may seek an appropriate protective order.

4.4 **Breach of the Confidentiality Covenants.** Compliance by each Party with requirements for use of Confidential Information shall not limit the breaching Party or its Representatives liability for any breach of its confidentiality obligations herein. In the event that the breaching Party or its Representatives breach the confidentiality covenants contained herein, the breaching Party recognizes that irreparable injury will result to the non-breaching Party or third parties entrusting Confidential Information to the non-breaching Party, that the non-breaching Party's remedy at law for damages will be inadequate, and that such Party will be entitled to an injunction to restrain the continuing breach by the breaching Party or its Representatives, or any other persons acting for or with the breaching Party. If the breaching Party is found, by a court of competent jurisdiction, to have breached the confidentiality covenants contained herein, the non-breaching Party shall be further entitled to recover:

- (a) actual, reasonable and provable damages to the non-breaching Party or its directors, officers, employees or agents;
- (b) any costs, losses or damages associated with any claims by third parties against the non-breaching Party;
- (c) reasonable attorneys' and other professionals' fees and all other costs and expenses incurred in connection with the non-breaching Party's enforcement of this Section 1.3 of the Agreement; and
- (d) any other rights and remedies with the non-breaching Party may have at law or in equity.

4.5 **Effect of Termination.** Unless otherwise provided herein, upon expiration or termination of the Agreement for any reason:

- (a) the limited right to use the Confidential Information granted to each Party under the Agreement will immediately terminate, and neither the Parties nor will their Representatives have any further right to use any Confidential Information in any way;
- (b) Supplier shall immediately return to Customer, or destroy at Customer's request, any developed software in source code and object code forms and all related documentation, all documents, drawings, models, apparatus, sketches, designs, source code, object code and any other tangible items containing any Confidential Information including all complete or partial copies, recordings, abstracts, notes or reproductions of any kind made from or about such tangible items or information contained therein; and
- (c) Supplier shall provide to Customer written certification, made under oath, that Supplier has returned or destroyed all of the items identified above to Customer, upon Customer's request. Notwithstanding the foregoing, the Receiving Party may retain copies of the Confidential Information for its use in connection with the prosecution or defense of any dispute arising from this Agreement, management and/or archival purposes.

5. **Data Processing and Data Security.** In the course of providing the Services to Customer, Supplier may Process Customer Personal Data (as defined in **Exhibit D**) on behalf of Customer. With respect to any Customer Personal Data Processed by Supplier in connection with the Services, Supplier agrees to comply with the terms and conditions set forth in **Exhibit D** (Data Processing and Data Security Addendum) attached hereto and incorporated herein by this reference.
6. **Insurance.**
- 6.1. During the term of this Agreement, any renewal terms or extensions of terms and conditions with respect to an uncompleted SOW pursuant to 9.1 herein (and, to the extent that any insurance is carried on a “claims made” basis, for such “tail” period thereafter that claims may be legally made with respect to occurrences during the term), Supplier shall have and maintain in force at least the following insurance coverage:
- (a) Workers’ Compensation with statutory limits required by the laws of each state exercising jurisdiction over Supplier engaged in performing Services under this Agreement.
 - (b) Employer’s Liability coverage with a minimum limit of one million dollars (\$1,000,000) for bodily injury by accident or disease.
 - (c) Commercial General Liability, including bodily injury, property damage, personal injury, advertising injury, products and completed operations, and contractual liability, in an amount not less than \$10,000,000 per occurrence and \$10,000,000 annual aggregate.
 - (d) Business Automobile Liability coverage (covering the use of all owned, non-owned and hired vehicles) for bodily injury (including death) and property damage with minimum limits (combined single limit) of one million dollars (\$1,000,000) per occurrence.
 - (e) Excess or Umbrella Liability coverage with a minimum limit of five million dollars (\$5,000,000) coverage in excess of Business Automobile Liability and Employer’s Liability.
 - (f) Employee Dishonesty (Fidelity) and Computer Crime coverage (for losses arising out of or in connection with any fraudulent or dishonest acts committed by employees of Supplier, acting alone or in collusion with others) with a minimum limit of ten million dollars (\$10,000,000) per wrongful act.
 - (g) Professional /Electronic Errors and Omissions/Cyber Liability Insurance covering acts, errors and omissions, negligence, breach of privacy perils as well as notification costs and regulatory defense, and network risks (including coverage for unauthorized access, failure of security), arising out of Consultant’s operations or services to which the insurance applies including coverage for computing implementation and development, design, execution, maintenance and follow-up work of computer programs whether application programs or software package, software and operations development work, implementation, testing, training, maintenance of software and systems and coverage for network and application services and any other activity directly or indirectly linked to information

technology and management consulting activities as well as arising out of any negligent act, error or omission committed by the Consultant while performing the foregoing functions for others and resulting in failure (i) to prevent unauthorized access with taking, obtaining, use or disclosure of data of customers or clients stored or processed in Consultant's computer or system; or (ii) to properly protect such data against a cyber-attack intentionally directed against Consultant, or, to prevent the transmission of such malware. Such insurance will be in an amount not less than \$10,000,000 per claim and in the policy term aggregate.

- 6.2. The foregoing coverages shall be maintained with insurers which have an A.M. Best rating of A- or better and /or an equivalent rating from a recognized insurance company rating agency.
- 6.3. Supplier's policies shall be primary and any insurance maintained by Customer shall be excess and noncontributory.
- 6.4. Except where prohibited by law, a Waiver of Subrogation as respects the Commercial General Liability, Business Automobile Liability and Workers Compensation/Employer's Liability policies will be included and will be noted on the Certificate of Insurance.
- 6.5. Supplier will include MoneyGram Payment Systems, Inc. and its Affiliates, officers, directors and employees as "additional insureds" for Commercial General Liability and Automobile and as a "loss payee" as to Employee Dishonesty (Fidelity) and Computer Crime.
- 6.6. Supplier shall cause its insurers or insurance brokers to issue certificates of insurance as set forth in section 6.5 above and deliver them to:

MoneyGram Payment Systems, Inc.
Attn: Global Supplier Excellence
2828 N. Harwood Street, Suite 1500
Dallas, TX 75201
SupplierManagement@moneygram.com

Supplier will use reasonable efforts to give thirty (30) days notice to Customer prior to cancellation or non-renewal of any of the policies providing such coverage.

7. **Disclaimers; Limitation of Liability.**

- 7.1. CUSTOMER UNDERSTANDS THAT SUPPLIER IS PERFORMING THE SERVICES HEREUNDER IN RELATION TO SYSTEMS AND DATA THAT HAVE BEEN PRODUCED BY OR SUPPLIED TO CUSTOMER BY THIRD PARTIES, AND FOR ALL OF WHICH SUPPLIER HAS NO RESPONSIBILITY. EXCEPT AS OTHERWISE STATED IN THIS SECTION 7.1, SUPPLIER MAKES NO WARRANTIES OF ANY KIND OR NATURE, WHETHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE OR USE, OR WARRANTIES OF ANY PRODUCTS OR SERVICES, OR THE APPROPRIATENESS OF CLIENT OR THIRD-PARTY SPECIFICATIONS. IN ADDITION, SUPPLIER EXPRESSLY DISCLAIMS ANY

WARRANTY OR LIABILITY WITH RESPECT TO DESIGN OR LATENT DEFECTS, SECURITY OF DATA OUTSIDE OF SUPPLIER'S MANAGED NETWORKS, OR COMPLIANCE WITH LAWS, REGULATIONS, OR OTHER OFFICIAL GOVERNMENT RELEASES APPLICABLE TO CUSTOMER, WHICH SHALL BE THE SOLE RESPONSIBILITY OF CUSTOMER.

7.2. Limitation of Liability. EXCEPT AS EXPRESSLY SET FORTH IN THE AGREEMENT, NEITHER PARTY WILL BE LIABLE FOR ANY INDIRECT, SPECIAL, INCIDENTAL, PUNITIVE, OR CONSEQUENTIAL DAMAGES, OR LOST PROFITS OF ANY KIND, IN CONNECTION WITH THE TERMS OR THE BREACH OF THE TERMS OR SUBJECT MATTER OF THE AGREEMENT, REGARDLESS OF THE FORM OF ACTION, WHETHER IN CONTRACT, TORT (INCLUDING NEGLIGENCE), STRICT LIABILITY, OR OTHERWISE, EVEN IF INFORMED OF THE POSSIBILITY OF SUCH DAMAGES IN ADVANCE. EITHER PARTY'S LIABILITY IN CONNECTION WITH THE AGREEMENT OR THE SUBJECT MATTER HEREOF, WILL NOT EXCEED, IN THE AGGREGATE, ONE MILLION U.S. DOLLARS (\$1,000,000 USD). NOTWITHSTANDING THE FOREGOING, THIS SECTION WILL NOT LIMIT A PARTY'S LIABILITY RESULTING FROM: (I) DEATH OR PERSONAL INJURY CAUSED BY IT OR ITS AGENTS' OR REPRESENTATIVES' NEGLIGENCE; (II) ITS GROSS NEGLIGENCE, WILLFUL MISCONDUCT, FRAUD, OR FRAUDULENT MISREPRESENTATION; OR FOR LIABILITY RESULTING FROM BREACH OF THE CONFIDENTIALITY OBLIGATIONS SET FORTH IN THE AGREEMENT; (IV) BREACH OF EXHIBIT D (DATA PROCESSING AND DATA SECURITY ADDENDUM); OR (IV) ANY LOSSES RECOVERABLE UNDER SECTION 8 (INDEMNIFICATION) A PARTY'S TOTAL LIABILITY IN THE AGGREGATE, FOR THE LIFE OF THE AGREEMENT WILL NOT EXCEED THE , IN THE AGGREGATE, FIFTEEN MILLION DOLLARS FOR AVOIDANCE OF DOUBT, SUPPLIER IS NOT LIABLE FOR ANY DAMAGES TO THE EXTENT RESULTING FROM CLIENT'S ACTIONS OR FAILURE TO COMPLY WITH THEIR OWN OBLIGATIONS.

7.3. Essential Element. The Parties agree that the limitations specified in this Section will survive and apply even if any limited remedy specified in the Agreement is found to have failed of its essential purpose.

8. **Indemnification.**

8.1. **Infringement Warranty/Indemnification.** Supplier will indemnify and hold Customer harmless from any action or claim and will defend at its expense any action brought against Customer that is based on a claim that Supplier did not have the right to enter into this Agreement or that the Services, or Deliverables, when used within the scope of this Agreement, infringe a patent or copyright or the trade secret or other proprietary rights of a third party (an "**Infringement**"). Supplier will pay any costs, damages, and reasonable attorneys' fees finally awarded against Customer in such an action, which are attributable to such claim. Should anything contemplated within the scope of this Agreement become, or in Supplier's opinion, is likely to become, the subject of a claim of Infringement,

Supplier may (a) procure for Customer the uninterrupted right to continue using the Deliverables (b) replace or modify the Deliverables to make them non-infringing; provided, however, that such replacement or modification shall, in any event, be capable of performing the equivalent functions as specified in the applicable SOW and compatible with Customer's existing systems and processes, or if neither (a) or (b) are possible, Supplier shall refund to Customer all fees paid by Customer under the applicable SOW and Customer shall be relieved from making any further payments. Supplier will have no Infringement indemnity obligation to the extent the claim of Infringement resulted directly from (i) Customer's combination, operation or use of the Deliverables any other products or processes with equipment, software or data not supplied, approved, authorized, or recommended by Supplier provided that such Infringement would not have occurred but for such combination or (ii) Supplier's compliance with any design specifications provided by Customer.

- 8.2. **Indemnification.** Each Party (the "Indemnifying Party") agrees to indemnify, defend, and hold harmless the other Party, their respective affiliates, and their respective employees, officers, directors, and other representatives (collectively, the "Indemnified Party") from and against any and all losses, costs, expenses (including reasonable fees and expenses for attorneys, experts, and consultants, and interest), penalties, fines, judgments, settlements, damages (of all types including special damages), or liabilities, including legal fees, costs, and expenses (collectively "Losses"), suffered or incurred by any of them in connection with any claim, cause of action, or other legal assertion, brought or threatened to be brought in a legal proceeding by a third party (who is not an affiliate or representative of the Indemnified Party), or any investigation, examination, or proceeding of a governmental agency (each a "Claim"), where such Claim is based on allegations as to any of the following: (i) a breach of the Indemnifying Party's representations and warranties under the Agreement; (ii) the gross negligence or willful misconduct of the Indemnifying Party; or (iii) any breach of **Exhibit D** (DATA PROCESSING AND DATA SECURITY ADDENDUM) resulting from the negligent acts or omissions of the Indemnifying Party. The Indemnified Party will give prompt notice of any Claims to the Indemnifying Party. An Indemnified Party may participate in the defense of any Claims by counsel of its own choosing, at its cost and expense. Neither Party will settle any Claims without the other Party's prior written approval, which will not be unreasonably withheld. The remedies in this Section are not exclusive and do not limit any other remedies a Party may have under the Agreement, Applicable Law, or otherwise.
- 8.3. **Supplemental Indemnification of Employment Claims.** Supplier agrees to fully defend, indemnify and hold harmless Customer from any investigation, claim, fine, taxes, or liability, brought by any government agency or entity, by any third party, or directly by any Personnel or subcontractor (a) arising or resulting from the employment of Personnel by Supplier, or its Affiliates or subcontractors (including liability for any social security or other employment Taxes and contributions applicable to the wages and salaries of such Personnel); (b) as a result of Supplier's payment or failure to pay any salary, wages, overtime pay, bonus or other cash compensation due and owing to any Personnel; (c) as a result of Supplier's offering or failure to offer any employee pension or other benefits of any Personnel; (d) as

a result of any other aspects of the employment relationship of Personnel with Supplier-or its Affiliates or the termination of such relationship, including claims for wrongful discharge, claims for breach of express or implied employment contract and claims of joint employment.

9. Representations and Warranties

9.1. Customer represents and warrants as follows:

- 9.1.1. Customer has all rights, titles and interests in, and has obtained all consents with respect to, all materials, data and software owned or developed by or licensed to Customer required for the performance of its obligations hereunder or to which access and use is required by Supplier, and that it has the authority and the legal right to permit Supplier to perform the services described in this Agreement or any SOW.
- 9.1.2. Customer warrants that the services it requests Supplier to provide will not violate the economic and trade sanctions administered by the Office of Foreign Assets Control ("OFAC") of the U.S. Department of Treasury. Client shall not disclose or provide access to any items which are subject to export control laws, regulations or restriction absent prior written agreement of the parties; in such case, Customer shall be the Exporter of Record and responsible for identifying to Supplier the export controlled items and obtaining any necessary licenses and/or approvals for disclosure to Supplier and for Supplier's onward disclosure to perform the services as contemplated in the SOW.

9.2. Supplier represents and warrants as follows:

- 9.2.1. **Performance.** The Services to be performed by Supplier shall be performed in a timely and professional manner. Supplier warrants that at the time of delivery to Customer, the Deliverables, when specified, will meet the applicable Specifications and shall be free from errors and from defects in workmanship and materials.
- 9.2.2. Any claim for breach of this performance warranty with respect to any of the Services must be made by written notice to Supplier within sixty (60) days of Customer's actual knowledge of the breach. For any such breach of this warranty, Customer's exclusive remedy, and Supplier's entire liability, shall be the re-performance of such Services, provided that if Supplier does not reperform the Services as so warranted under this Section 8, Customer shall be entitled to recover the fees paid to Customer for such deficient Services. **Solvency.** Supplier warrants that it is financially solvent and has the ability to perform its obligations under this Agreement.
- 9.2.3. **Compliance with Laws.** Supplier warrants and represents that it is a business entity in good standing and duly authorized to do business and perform its obligations under this Agreement. Supplier will comply with all applicable federal, state, international and local laws in meeting its obligations under this Agreement that apply to Supplier in the ordinary course of its business as an IT services provider (i.e. independently of its performance of this Agreement).

- 9.2.4. **Licenses.** Supplier will maintain and cause its agents to maintain during the term of this Agreement all licenses and permits, if any, required to carry out Supplier's obligations under this Agreement.
- 9.2.5. **Fiduciary Standards and Conflict of Interest.** Supplier warrants that in the performance of Supplier's duties under this Agreement, Supplier shall adhere to the highest fiduciary standards, ethical practices and standards of care and competence.
- 9.2.6. **Warranty against Disablement.** Supplier warrants that no portion of any media provided to Customer contains or will contain any protection feature designed to prevent its use. This includes, without limitation, any computer virus, worm, software lock, drop dead device, Trojan-horse routine, trap door, time bomb or any other codes or instructions that may be used to access, modify, delete, damage or disable Customer's systems.
- 9.2.7. **Warranty of Title.** Supplier warrants that it owns and has the right to license or convey title to any Created Works, Deliverables, documentation and other materials covered by this Agreement. Supplier will not grant to any third party any rights or licenses to any intellectual property or technology that would conflict with Supplier's obligations or Customer's rights under this Agreement.
- 9.2.8. **Litigation.** Supplier warrants and represents that it is not a party to any pending litigation the resolution of which is reasonably likely to affect adversely the ability of Supplier to fully perform its obligations hereunder, nor is any such litigation reasonably contemplated or threatened. Supplier agrees to inform Customer in the event any such litigation occurs or becomes reasonably contemplated during the term of this Agreement.
- 9.2.9. **Anti-Bribery/Anti-Corruption.** The Parties agree that **Exhibit E**, Anti-Bribery/Anti-Corruption Representations, Warranties and Covenants, attached hereto and incorporated herein by this reference, shall apply to the Parties performance and obligations under this Agreement.
- 9.2.10. **OFAC.** Supplier represents and warrants that none of its subsidiaries or, to its knowledge, any director, officer, employee, consultant, subcontractor or agent of Supplier, or any of its subsidiaries is an individual or entity ("Person") who (a) is directly or indirectly owned or controlled by any Person currently included on (i) the List of Specially Designated Nationals and Blocked Persons or the Foreign Sanctions Evaders List (collectively, "SDN List") maintained by the Office of Foreign Assets Control, U.S. Department of the Treasury ("OFAC") at <https://www.treasury.gov/resource-center/sanctions/SDN-List/Pages/default.aspx> and as may be amended from time to time; or (ii) any international governmental or non-governmental entity list such as the United Nations Security Council, the European Union, and Her Majesty's Treasury (UK) (collectively "Governmental or Non-Governmental Entity") imposing economic sanctions and trade embargoes ("Economic Sanctions Laws"); or (b) is directly or indirectly owned or controlled by any Person who is located, organized, or resident in a country or territory that is, or whose government is, the target of sanctions imposed by OFAC or any other Governmental or Non-Governmental Entity. Supplier shall promptly notify Customer when it or any of its subsidiaries, or any of its subsidiaries' directors, officers, employees, consultants, subcontractors or agents become directly or indirectly owned or controlled by any Person (a) included on the then-current SDN List or any other Governmental or Non-

Governmental Entity list; or (b) located, organized, or resident in a country or territory that is, or whose government is, the target of sanctions imposed by OFAC or any other Governmental or Non-Governmental Entity

10. **Term and Termination.**

10.1. **Term of Agreement.** This Agreement shall commence on the effective date of this Agreement and shall continue in effect for one year. Thereafter, this Agreement shall automatically renew for additional one (1) year periods (“**Renewal Term**”), unless a Party gives written notice of its intent not to renew this Agreement to the other Party at least thirty (30) days before the expiration of the original term or any Renewal Term. However, if any SOW, which has been duly executed by the authorized representative of each Party, specifies that all or part of Supplier’s performance for the SOW(s) shall occur after the expiration or termination date of this Agreement, then the terms and conditions of this Agreement shall continue to govern the Parties’ performance until the obligations under the Agreement and such SOW have been completely discharged.

10.2. **Termination by Customer Without Cause.** Unless otherwise stated in the applicable SOW, Customer may elect, at its sole discretion, to terminate this Agreement or any SOW (in whole, or in part) by providing Supplier not less than 30 day notice. Notice of termination of a SOW under this section shall be given in writing. The notice should specify the last day that services will be performed under the SOW (the “**Last Working Day**”) and Customer will not be liable to Supplier for payment in connection with any services performed after the Last Working Day.

10.3. **Termination by Customer for Cause.** If Supplier breaches any provision of this Agreement and such breach is not cured within thirty (30) days after written notice thereof to Supplier, Customer may elect to terminate this Agreement or the applicable SOW effective immediately.

10.4. **Termination by Supplier for Cause.** If Customer breaches any provision of this Agreement, and such breach is not cured within thirty (30) days after written notice thereof to Customer, Supplier may elect to terminate this Agreement or any outstanding SOW effective immediately. If this Agreement is terminated by Supplier under this Section 9.4 and Supplier is not in breach of this Agreement, Customer will pay undisputed invoice amounts within thirty (30) days of Invoice Date for all Services rendered through the date of such termination unless payment is waived under Section 2, above. All disputed invoices will be handled in accordance with Section 12.19, the Dispute Resolution provision of the Agreement.

11. **Notices.** Any notice permitted or required by this Agreement must be in writing and shall be deemed given when sent by mail or courier and addressed as follows:

If to Customer: **Contract Lifecycle Management**
MoneyGram Payment Systems, Inc.
2828 N. Harwood Street, Suite 1500
Dallas, TX 75201
Contracts@moneygram.com

With copies to: **Office of the General Counsel**
MoneyGram Payment Systems, Inc.



Attn: Robert Villaseñor, EVP, General Counsel & Secretary
M.S. DAL-TX01
2828 N. Harwood Street, Suite 1500
Dallas, TX 75201

If to Supplier: Capgemini America, Inc.
79 Fifth Avenue, 3rd Floor
New York, NY 10003
Attention: General Counsel

12. **Miscellaneous.**

- 12.1. **Relationship of the Parties.** This Agreement shall not be interpreted to create, nor is it intended to create, any joint venture, partnership, agency, employment relationship or other joint enterprise between Supplier and Customer. Supplier shall take all actions and do all things which are required to comply with all laws respecting its position as an independent contractor providing Services pursuant to this Agreement. In making and performing this Agreement, the Parties shall act at all times as independent contractors, and at no time shall either Party make any commitments or incur any charges or expenses for or in the name of the other Party.
- 12.2. **Policies.** Whenever Supplier is present on the Customer's premises, Supplier shall comply with all Customer policies and procedures governing on-site work, including the Customer's safety, security and data protection policies and procedures, and all reasonable instructions and directions issued and provided by the Customer to Supplier. To the extent any of Customer's applicable policies are written in such a way as to apply only to Customer's employees, Supplier shall nonetheless be obligated to comply with the spirit and intent of such policies.
- 12.3. **Removal of Personnel.** If at any time Customer asks Supplier to remove any Personnel from any Customer facility or from performing any portion of the Services due to misconduct or poor work performance, Supplier will promptly do so upon receiving written request with Customer's reasoning. Any Personnel who have been removed from performing any portion of the Services for any performance-based or conduct-based reason shall not be re-assigned by Supplier to perform any further work for Customer whatsoever, absent Customer's prior written consent. Customer will not be required to pay for any portion of the Services that were performed in an unsatisfactory manner by such replaced Personnel or for the time spent to train or orient replacement Personnel.
- 12.4. **Non-Competition.** Supplier shall not assign any Personnel who perform any portion of the Services for Customer to perform work for the benefit of Euronet Worldwide, Inc. and its affiliates, or Western Union and its affiliates, within one year after such Personnel's assignment to Customer has terminated, unless Customer has expressly agreed otherwise in writing.
- 12.5. **Employment Laws.** Supplier shall follow all applicable employment laws. Supplier shall not engage in any unlawful discrimination based on race, color, religion, sex, national origin, age, disability, genetic information, family medical history, or any other criteria

prohibited by applicable law, in any employment or staffing decision related to the provision of Services under this Agreement. Supplier shall provide, at Supplier's sole expense, any reasonable accommodations needed to permit qualified Personnel to perform the essential functions of any assignment. Supplier shall assume sole responsibility for compliance with all applicable Family and Medical Leave Act obligations relating to Personnel.

- 12.6. **Employment Taxes and Benefits.** Supplier shall pay all wages and employment taxes and make all withholdings required by law for the Personnel. Supplier is solely responsible for payment and withholding of any and all Social Security taxes, Medicare taxes, unemployment taxes, and federal and state and local taxes and withholdings for Personnel. Supplier is solely responsible for reporting to the appropriate governmental agencies all payments made to, and withheld from, all Personnel supplied by Supplier for any work performed for the benefit of Customer.
- 12.7. **Fair Labor Standards Act.** With respect to the Personnel, Supplier is solely responsible for ensuring compliance with the Fair Labor Standards Act and all other applicable federal, state, and local wage and hour laws, including all laws related to the payment of overtime, minimum wage, child labor laws, and meal and rest breaks. Supplier is solely responsible for maintaining all timekeeping records for Personnel as may be required under applicable law.
- 12.8. **Workers' Compensation.** Supplier is solely responsible for maintaining workers' compensation coverage sufficient to cover any injury to Personnel while working on any matter for Customer. Supplier accepts responsibility, through workers' compensation, for any compensable injury to Personnel while working on any matter for Customer. Supplier agrees to indemnify and hold Customer harmless in the event of any negligence claim or other claim by Personnel, if such claim arguably would have been covered under workers' compensation laws had the injury been to an employee of Customer. Supplier shall waive any subrogation rights against Customer for workers' compensation benefits and shall obtain a waiver from any insurance carriers with whom Supplier carries workers' compensation insurance releasing their subrogation rights against Customer.
- 12.9. **Governing Law and Venue.** This Agreement will be construed and enforced in accordance with and governed by the laws of the State of Texas; provided, that laws regarding conflicts of laws will not defeat application of the substantive laws of the state of Texas. The Parties agree to the personal jurisdiction of the State of Texas. The jurisdictional venue for any proceedings involving this Agreement shall be Dallas County, Texas.
- 12.10. **Integration.** This Agreement and the SOW(s) (which are incorporated herein by reference and made a part hereof) set forth the entire agreement and understanding of the Parties in respect of the transactions contemplated hereby and supersede all prior agreements, arrangements and understandings, whether written or oral, relating to the subject matter hereof. Except as expressly set forth herein, no other prior or contemporaneous covenants, promises, representations or warranties of any kind, whether written or oral, have been made or can be relied on by either party as an inducement to enter into this Agreement, whether relating to the tools, resources, practice or otherwise of any party hereto.

- 12.11. **Assignment.** Neither party may assign this Agreement without the prior written consent of the other party. This Agreement shall be binding upon, and inure to the benefit of, the successors and permitted assigns of the parties hereto.
- 12.12. **Non-Exclusive.** Nothing in this Agreement is intended to restrict Customer from entering into similar agreements with third parties.
- 12.13. **Waiver.** Failure of either Party to object to any act or omission of the other Party, no matter how long the same may continue, shall not be deemed to be a waiver by such Party of any of its rights hereunder. No waiver by any Party at any time of any other provision of this Agreement shall be deemed a waiver or breach of any other provision of this Agreement or consent to any subsequent breach of the same of any other provision hereunder. If any act or omission by any Party shall require the consent or approval of another Party, such consent or approval of such act or omission on any one occasion shall not be deemed a consent to or approval of said act or omission on any subsequent occasion or consent to or approval of any other act or omission on the same or any subsequent occasion. Waiver of any rights or remedies must be in a signed writing by the waiving Party.
- 12.14. **Modifications.** This Agreement may not be modified, changed or supplemented, nor may any obligations hereunder be waived or extensions of time for performance granted, except, by written instrument signed by authorized representatives of both Parties.
- 12.15. **Counterparts.** This Agreement may be executed simultaneously in multiple counterparts, each of which shall be deemed an original, but all of which taken together shall constitute one and the same instrument. In the event that any signature is delivered by facsimile transmission or by e-mail delivery of a ".pdf" format data file, such signature shall create a valid and binding obligation of the party executing (or on whose behalf such signature is executed) with the same force and effect as if such facsimile or ".pdf" signature page were an original thereof.
- 12.16. **Headings.** The paragraph headings contained in this Agreement are for convenient reference only, and shall not in any way affect the meaning or interpretation of this Agreement.
- 12.17. **Severability.** If any provision of this Agreement is held to be illegal, invalid or unenforceable under present or future laws effective during the term hereof, such provision shall be fully severable; this Agreement shall be construed and enforced as if such illegal, invalid or unenforceable provision had never comprised a part hereof; and the remaining provisions of this Agreement shall remain in full force and effect and shall not be affected by the illegal, invalid or unenforceable provision or by its severance from this Agreement. Furthermore, in lieu of each such illegal, invalid or unenforceable provision, there shall be added automatically as a part of this Agreement a provision as similar in terms to such illegal, invalid or unenforceable provision as may be possible and be legal, valid and enforceable.
- 12.18. **Force Majeure.** Neither Party to this Agreement shall be liable for failure to perform or delay in performance of any of its obligations under this Agreement (except payment of amounts already due and owing) where such failure or delay results from any act of God, pandemic, military operation, catastrophic event directly related to terrorist activity, national emergency, civil commotion, or utility, or the order, requisition, request or

recommendation of any government agency or acting government authority, or any Party's compliance therewith, or government probation, regulation, or priority, or any change in laws or regulations which prevent any Party from providing services required by this Agreement, or any other cause beyond any Party's reasonable control whether similar or dissimilar to the foregoing causes. In the event said force majeure event causes a delay that lasts more than ten (10) days, Customer has the right to terminate this Agreement without further obligation, financial or otherwise, except for non-financial obligations which expressly survive the termination of this Agreement. In addition, Supplier shall return any monies paid by Customer for products or services not delivered.

- 12.19. **Attorneys' Fees.** If any dispute arises between the parties regarding any Party's rights or obligation pursuant to this Agreement, the prevailing Party will be entitled to reasonable attorneys' fees, attorneys' costs, expert witness fees, and arbitration or court costs incurred in connection with such litigation.
- 12.20. **Survival.** Any provisions of this Agreement which requires performance or grants a benefit after termination of the Agreement shall be deemed to survive the termination of the Agreement. Expiration or termination of the Agreement shall not terminate any outstanding SOW, which SOW shall remain in effect until terminated itself in accordance with this Agreement, and/or the applicable SOW. The Agreement shall remain in effect with respect to any outstanding SOW, as to which this Agreement will terminate on completion thereof.
- 12.21. **Interpretation.** This Agreement shall be fairly interpreted in accordance with its terms and without any strict construction in favor of or against either Party. Any ambiguity shall not be interpreted against the drafting Party.
- 12.22. **Use of Name.** Supplier agrees not to refer to Customer directly or indirectly in any promotion or advertisement, metatag, news release or release to any general or trade publication or any other media.
- 12.23. **Export/Re-export Compliance.** The Parties acknowledge that the exportation from the United States of materials, products and related technical data (and the re-export from elsewhere of United States origin items) may be subject to compliance with United States export laws, including, without limitation, the United States Bureau of Export Administrations Export Administration Regulations and the United States Department of States International Traffic and Arms Regulations which restrict export, re-export, and release of materials, products and their related technical data, and the direct products of such technical data. The Parties agree to comply with all exports Laws and to commit no act that, directly or indirectly, would violate any United States law, or any other international treaty or agreement, relating to the export, re-export, or release of any materials, products or their related technical data to which the United States adheres or with which the United States complies.
- 12.24. **Non-Discrimination.** The Parties incorporate by reference the provisions of the equal opportunity clauses of Executive Order 11246, 41 CFR 60-1.4(a); the Vietnam Era Veterans Rehabilitation and Adjustment Act, 41 CFR 60-250.5(a); and Section 503 of the Rehabilitation Act, 41 CFR 60-741.5(a).
- 12.25. **Dispute Resolution; Equitable Relief.**



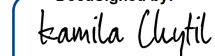
- 12.25.1. The Parties will attempt in good faith to resolve any controversy or claim arising out of or relating to this Agreement or the Services through discussions between the Capgemini Vice President and the senior leader on behalf of Client responsible for providing and accepting the Services. If these discussions are unsuccessful, The Parties agree that any action asserting a claim by one party against the other party hereto arising out of or relating to this Agreement or the Services must be brought in the state or federal court for the county or district wherein the party against which the claim is brought has its principal place of business. Notwithstanding the foregoing, any action asserting a claim for collection of fees, expenses and/or other compensation due or owing to Capgemini under this Agreement may be brought in a state or federal court in Dallas, Texas. If an action is pending on any claims between the Parties, any claim which could be brought as a counterclaim must be brought in the pending action, if at all. The Parties further agree to waive any right to a jury trial that either party might otherwise have in any and all courts.
- 12.25.2. The Parties acknowledge that the breach of Confidentiality, by one party will give rise to irreparable injury to the other Party which is not adequately compensable in damages or at law. Accordingly, the Parties agree that injunctive relief will be an appropriate remedy to prevent violation of either Party's respective rights and/or obligations thereunder.
- 12.26. **Customer Responsibility:** Customer will provide Supplier with reasonable and legal access to and use of the systems, data, software and premises necessary for the performance of the services, as applicable. Customer agrees that Supplier's Personnel will connect only through the Customer provided virtual desktop environment and Customer will configure VDI to restrict access or storage of data on Supplier's Personnel endpoint device (e.g., copy/paste, drive mapping, etc). Customer has implemented data leakage prevention on systems used by Supplier's Personnel to prevent accidental data loss by such Personnel. Customer represents and warrants that it has all rights, titles and interests in, and has obtained all consents with respect to, all materials, data and software owned or developed by or licensed to Customer required for the performance of its obligations hereunder or to which access and use is required by Customer, and that it has the authority and the legal right to permit Customer to perform the services described in the SOW and contemplated thereby. Customer warrants that the services it requests Supplier to provide will not violate the economic and trade sanctions administered by the Office of Foreign Assets Control ("OFAC") of the U.S. Department of Treasury. Client shall not disclose or provide access to any items which are subject to export control laws, regulations or restriction absent prior written agreement of the Parties; in such case, Customer shall be the Exporter of Record and responsible for identifying to Supplier the export controlled items and obtaining any necessary licenses and/or approvals for disclosure to Supplier and for Supplier's onward disclosure to perform the services as contemplated in the SOW.
- 12.27. **Solicitation.** During the term of a SOW and for a period of one (1) year following its termination, neither party shall, as a result of becoming aware of any employee of the other party or its subcontractors who is connected with the performance of such SOW, directly or indirectly solicit or hire (or utilize as an independent contractor) such employee.



IN WITNESS WHEREOF, the Parties hereto have executed this Agreement.

MoneyGram Payment Systems, Inc.

DocuSigned by:



Signature

Kamila Chytil

By: Name

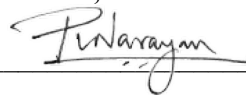
Chief Operating Officer

Its: Title

10-Sep-2020

Date

Capgemini America, Inc.



Signature

Narayan Puthanmadhom

By: Name

EVP

Its: Title

09/03/20

Date


EXECUTION VERSION
Office of General Counsel

September 3, 2020

EXHIBIT A
SAMPLE STATEMENT OF WORK

STATEMENT OF WORK

This Statement of Work (“**Statement of Work**” or “**SOW**”) adopts and incorporates by reference the terms and conditions of the Business Services Master Agreement (“**Master Agreement**”), which was entered into on August 20, 2020, between Capgemini America, Inc., with its principal offices located at 79 Fifth Avenue, 3rd Floor, New York, NY 10003 (“**Supplier**”) and MoneyGram Payment Systems, Inc., a Delaware corporation (“**Customer**”), as it may be amended from time to time. Customer and Supplier are jointly referred to as the “**Parties**”, and each, a “**Party**.” This SOW is effective beginning on [DATE] (“**Effective Date**”) and will remain in effect until [DATE/CONTINGENCY] (“**Expiration Date**”), unless earlier terminated in accordance with the Master Agreement. Transactions performed under this SOW will be conducted in accordance with and be subject to the terms and conditions of this SOW, the Master Agreement, and any applicable purchase order (“**PO**”). This SOW is not a PO. Capitalized terms used but not defined in this Statement of Work shall have the meanings set out in the Master Agreement.

1. Defined Terms: For purposes of this SOW, the following terms shall have the following meanings:

"[DEFINED TERM]" [TEXT OF DEFINITION].

"[DEFINED TERM]" [TEXT OF DEFINITION].

2. Scope of Work: [PROJECT SUMMARY].
3. Specification: [DETAILED DESCRIPTION OF THE SERVICES AND/OR PRODUCTS TO BE PROVIDED].
4. Deliverables and Work Schedule: The relevant Deliverables, work schedules, milestones, completion dates, and related terms associated with this SOW are set forth herein.

- 4.1 Deliverables: The relevant Deliverables associated with this SOW are as follows:

Line Item	Quantity	[Good/Product] [or other] [Deliverable]	Delivery Date	Delivery Location
1.				
2.				
3.				

- 4.2 Work Schedule: The relevant tasks, milestones and completion dates are as follows:

Line Item	Task	Completion Date
1		
2		
3		

[For Services which contemplate the delivery of fixed priced, project based work and timely delivery is critical to the overall success of the project (e.g. software development services, system or application implementation, etc.), the Contract Manger may consider incorporating language here which provides for credits should Supplier fail to complete the project deliverables by the stated dates. For suggested language, please contact Legal.]

5. Personnel: [NAME AND/OR TITLE/SKILL LEVEL AND HOURLY RATE. SEE [SECTION 1.2(c)*]] [*ALL REFERENCED SECTIONS IN THE SOW TEMPLATE WILL NEED TO BE REVIEWED AND ALIGNED WITH THE APPROPRIATE SECTIONS IN THE APPLICABLE MASTER AGREEMENT.]
6. Pricing [Time and Materials Estimate]: [ESTIMATE IN US DOLLARS OF ALL TIME, MATERIALS AND EXPENSES, ASSUMPTIONS, DEPENDENCIES OR LIMITATIONS. SEE SECTION [1.2(e)(i)]]. [Fixed Fee]: [STATE FEE AMOUNT IN US DOLLARS, MATERIALS TO BE PROVIDED, WHETHER TRAVEL OR OTHER EXPENSES ARE INCLUDED AND ANY ASSUMPTIONS, DEPENDENCIES OR LIMITATIONS. [SEE SECTION [1.2 (e)(ii)]]].

Item	Price [Per Unit/[Other]]	[Cost Structure]
Total:		

[SUGGESTED LANGUAGE TO INCLUDE WHEN TRAVEL AND RELATES EXPENSES ARE ANTICIPATED: *Travel and related expenses must be preapproved in writing by Customer prior to Supplier making the expense, and will be reimbursed to Supplier with the appropriate support documentation. In incurring travel and related expenses, Supplier shall conform to Customer's travel policies and procedures. Supplier will not charge Customer for travel time for pre-approved trips.*]

7. Assistance by Customer: [SEE SECTION [1.2(d)]]
8. Key Persons: The following are Key Persons as identified under Section [1.2(g)] the Master Agreement: [IDENTIFY ANY SUPPLIER PERSONNEL WHO ARE KEY AS DEFINED IN SECTION [1.2(g)]]].
9. Subcontractors: The following subcontractors are permitted under Section [1.2(h)] of the Master Agreement: [SUBCONTRACTOR NAMES] [IDENTIFY ANY SUBCONTRACTORS WHO HAVE BEEN APPROVED BY CUSTOMER PER SECTION 1.2(h)]
10. Other SOW-Specific Terms and Conditions: [SOW-SPECIFIC TERMS AND CONDITIONS].
11. Acceptance Criteria: [IDENTIFY ANY SPECIFIC ACCEPTANCE CRITERIA IN ADDITION TO THOSE LISTED UNDER SECTION [2.3], IF ANY.] [SAMPLE LANGUAGE: Upon completion of each Deliverable, Supplier will deliver the Deliverable to Customer in accordance to the terms set forth in this SOW and the Master Agreement. If requested by Customer, Supplier

will provide a walkthrough of the content of each Deliverable. Customer will provide sign off in writing its acceptance or rejection of a Deliverable. If Customer rejects a Deliverable, Customer will provide Supplier a complete list of deficiencies in the rejected Deliverable. Supplier will promptly address and correct these deficiencies so that the applicable Deliverables will materially conform to the specifications set forth in this SOW and resubmit the Deliverable for Customer's review and acceptance. Customer shall then review the resubmitted Deliverable and confirm its acceptance of the Deliverable by providing Supplier a written sign off. Deliverables such submitted will be deemed accepted if no return notice of rejection of the applicable Deliverable is provided to Supplier within fifteen (15) business days of final submission thereof.]

12. Services Coordination: Each Party designates the following persons as authorized representatives assigned to serve as the primary point of contact for communication, issue escalation, contract administration, acceptance of Deliverables as set forth herein, and other related matters.

Customer's Authorized Representative	Email Address
Supplier's Authorized Representative	Email Address

13. Change Management Procedure: The scope of work, specification, Deliverables, pricing, and other terms specified in this SOW shall not change in any material aspect, except where approved by both Parties using the following process:

- 14.1 Review Process. The Supplier and Customer authorized representatives will review an issue and determine mutually that a resolution will lead to a change in scope, defined as a change that will have material impact on work scope, key tasks, work schedule, deliverables, acceptance criteria, cost, staffing, or other terms of the SOW.
- 14.2 Change Request. The proposed change is documented in a written project change request ("Change Request"), including the impact on project scope, work schedule, cost and so forth. The Change Request shall be made in the format attached to this SOW, as Exhibit [X].
- 14.3 Approval and Signature. The Change Request is reviewed by the applicable Customer program lead, and approved by obtaining the signature of authorized representatives of Customer and Supplier on the Change Request form. A Change Request is signed by both Parties and becomes part of this SOW by this reference herein.
14. Supplier Performance: If all or part of Supplier's performance under this SOW occurs after the expiration or termination date of the Master Agreement, then the terms and conditions of the Master Agreement shall continue to govern the Parties performance until the obligations under the Master Agreement and this SOW have been completely discharged.
15. Integration: This SOW is the final, complete, and exclusive agreement of the Parties with respect to the subject matters hereof and supersedes all prior discussions and agreement between the Parties with respect to such subject matters. No modification of or amendment to this SOW, or any waiver of any rights under this SOW will be effective unless in writing and signed by both Parties.

IN WITNESS WHEREOF, the Parties hereto have executed this SOW the date first above written.

MoneyGram Payment Systems, Inc.

[SAMPLE, DO NOT SIGN]

Signature

Signature

By: Name

By: Name

Its: Title

Its: Title

Date

Date

EXHIBIT B**DRUG SCREENING PROTOCOL**

- Initial screen of urine specimens will be by immunoassay (“EMIT”).
- Presumptive positive urine specimens will be confirmed by gas chromatography/mass spectrometry (“GC/MS”).
- Each urine specimen will be assayed for the presence of the following compounds at the detection levels indicated.

SAP 7 Panel

DRUG GROUP	EMIT SCREEN DETECT LEVEL* ng/ml**	GC/MS CONF DETECT LEVEL* ng/ml**
Amphetamines	1000	500
Cocaine Metabolites	300	150
Marijuana Metabolites	50	15
Opiates Metabolites	2000	2000
Phencyclidine	25	25
Benzodiazepine	300	200
Barbiturates	300	200

* The detection levels indicated represent the lowest cutoff concentration for an analyte within that class. Actual cutoff levels for other analytes within the class may be higher.

** nanogram/milliliter

Each urine specimen will also be assayed for signs of possible adulteration. Specimen adulteration assays will consist of two or more of the following:

- Creatinine
- Nitrites
- pH

EXHIBIT C**ACKNOWLEDGEMENT
OF IP OWNERSHIP AND CONFIDENTIALITY OBLIGATIONS**

This ACKNOWLEDGEMENT OF IP OWNERSHIP AND CONFIDENTIALITY OBLIGATIONS ("Exhibit") supplements and forms part of the Agreement entered into by and between Customer and Supplier. Capitalized terms not otherwise defined herein shall have the meaning given to them in the Agreement.

1. IP Ownership

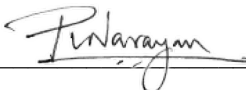
In accordance with Section 3, Ownership, of the Agreement, Supplier acknowledges that Supplier is to assign to Customer any and all rights, title and interest, including, without limitation, copyrights, trade secrets and proprietary rights, to the materials created by Supplier specifically for Customer hereunder and required to be delivered to Customer by virtue of their description or specification as a Deliverable in an applicable SOW.

2. Confidentiality

Supplier hereby acknowledges the obligations of Section 4, Confidentiality, in the Agreement and agrees to act in accordance with the Section and inform Supplier Personnel of the obligations.

ACKNOWLEDGED AND AGREED TO THIS ____ DAY OF _____, 20__.

Capgemini America, Inc.



Signature

Narayan Puthanmadhom

By: Name

EVP

Its: Title

09/03/20

Date

EXHIBIT D**DATA PROCESSING AND DATA SECURITY ADDENDUM**

This DATA PROCESSING AND DATA SECURITY ADDENDUM (“**Addendum**”) supplements and forms part of the Agreement entered into by and between Customer and Supplier. Capitalized terms not otherwise defined herein shall have the meaning given to them in the Agreement.

1. **Definitions.**

- 1.1 “**Controller**” means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the Processing of Personal Data; where the purposes and means of such processing are determined by European Union or Member State law, the controller or the specific criteria for its nomination may be provided for by the European Union or Member State law.
- 1.2 “**Customer Personal Data**” means any Personal Data which is provided to, or accessed by, Supplier by or at the direction of Customer and that is Processed by Supplier on behalf of Customer.
- 1.3 “**Data Subject**” means an individual who is the subject of Personal Data.
- 1.4 “**EU Data Protection Laws**” means EU Directive 95/46/EC, as transposed into domestic legislation of each Member State and as amended, replaced or superseded from time to time, including by the GDPR and laws implementing or supplementing the GDPR.
- 1.5 “**GDPR**” means the EU General Data Protection Regulation 2016/679.
- 1.6 “**CCPA**” means the California Consumer Privacy Act of 2018.
- 1.7 “**Personal Data**” means any data that identifies, relates to, is capable of being associated with, or could reasonably be linked to an identified or identifiable natural person or household. An identifiable natural person or household is one that can be identified, directly or indirectly, by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person or household.
- 1.8 “**Data Protection Laws**” means EU Data Protection Laws and, to the extent applicable, the CCPA and the data protection or privacy laws of any other country.
- 1.9 “**Processing, Processes, Processed or Process**” means any operation or set of operations which are performed on Personal Data or on sets of Personal Data, whether or not by automated means, such as, collecting, recording, organizing, structuring, storing, adapting or altering, retrieving, consulting, using, disclosing, disseminating or otherwise making available, restricting, erasing, destroying Customer Personal Data.
- 1.10 “**Processor**” means a natural or legal person, public authority, agency or any other body which Processes Personal Data on behalf of the Controller. A service provider under CCPA is considered a Processor for purposes of this Addendum.

- 1.11 “**Restricted Transfer**” means: (i) a Transfer of Customer Personal Data from Customer to Supplier; or (ii) an onward Transfer of Customer Personal Data from Supplier to a Subprocessor, in each case, where such transfer would be prohibited by Data Protection Laws (or by the terms of data transfer agreements put in place to address the data transfer restrictions of Data Protection Laws) in the absence of the Standard Contractual Clauses to be established under Section 5.
- 1.12 “**Security Breach**” means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Customer Personal Data transmitted, stored or otherwise processed on systems under the direct control of Supplier.
- 1.13 “**Standard Contractual Clauses**” means the contractual clauses set out in **Schedule A** to this Exhibit D, amended as indicated (in square brackets and italics) in that Schedule.
- 1.14 “**Subprocessor**” means any third party appointed by or on behalf of Supplier to Process Customer Personal Data that does not collect Personal Data from the Data Subject or act as a contracted Processor on behalf of the Controller.
- 1.15 “**Transfer**” means to disclose or otherwise make Personal Data available to a third party (including to any Subprocessor), either by physical movement of the Personal Data to such third party or by enabling access to the Personal Data by other means.

2. **Data Processing.**

- 2.1 In the context of Supplier’s Processing of Customer Personal Data, Supplier shall act as Processor to Customer who will act as the Controller with respect to Customer Personal Data.
- 2.2 Supplier shall: (a) comply with all applicable Data Protection Laws in the Processing of Customer Personal Data, including, but not limited to, security, record keeping, notifying Controller of data breaches, and restrictions on international data transfers; (b) assist Customer comply with applicable Data Protection Laws; and (c) not Process Customer Personal Data other than on Customer’s documented instructions. Supplier must promptly notify Customer if, in its opinion, Customer’s instructions would not comply with the Data Protection Laws or any other applicable law. Further, Supplier must promptly comply with any Customer request or instruction, requiring Supplier to amend, transfer, or delete Customer Personal Data, or to stop, mitigate, or remedy any unauthorized Processing.
- 2.3 Supplier agrees and covenants that it shall: (a) keep and maintain all Customer Personal Data in strict confidence, using such degree of care as is appropriate to avoid unauthorized access, use, or disclosure; (b) not create, collect, receive, access, or use Customer Personal Data in violation of law; (c) use and disclose Customer Personal Data solely and exclusively for the purposes for which the Customer Personal Data, or access to it, is provided pursuant to the terms and conditions of this Addendum and Agreement, and not use, sell, rent, transfer, distribute, or otherwise disclose or make available Customer Personal Data for Supplier's own purposes or for the benefit of anyone other than Customer, in each case, without Customer's prior written consent; and (d) not, directly or indirectly, disclose, delete, or provide access to, Customer Personal Data to any person other than its

authorized employees and representatives, without Customer's prior written consent or as required by applicable Data Protection Laws.

- 2.4 All of Supplier's employees and representatives who Process Customer Personal Data shall: (a) be informed of the Customer Personal Data's confidential nature and use restrictions; (b) have undertaken training on the Data Protection Laws relating to handling Personal Data and how it applies to their particular duties; (c) be aware both of Supplier's duties and their personal duties and obligations under the Data Protection Laws and this Addendum. All of Supplier's employees and representatives who Process Customer Personal Data must have agreed in writing, via an employment agreement or other contractual document, to maintain the confidentiality.
- 2.5 Taking into account the nature of the processing and insofar as it is possible, Supplier will assist Customer respond to requests by individuals exercising their rights under applicable Data Protection Laws. These obligations include Data Subject's rights that may include, but not limited to, the ability to: (a) access his/her Personal Data held by Customer; (b) request corrections to or erasure of his/her Personal Data held by Customer; and (c) seek to restrict Processing of his/her Personal Data by Customer. Supplier must promptly notify Customer if it receives a request from a Data Subject for access to their Personal Data, or if Supplier receives any complaint, notice, or communication that directly or indirectly relates to the Personal Data Processing or to any Party's compliance with the Data Protection Laws.
- 2.6 Unless otherwise agreed to the contrary, Supplier will, at the request of Customer or within 180 days of the expiration or termination of the Agreement, destroy or deliver to Customer (and shall cause its agents and subcontractors to destroy or deliver) all materials containing Customer Personal Data, together with any and all copies thereof (excluding archived or other copies that are not readily retrievable and are scheduled for deletion pursuant to an established Supplier retention schedule, which shall be provided to Customer and provided such scheduled deletion subsequently takes place). Notwithstanding the foregoing, Supplier may retain one archived copy of any information that it is required by law to retain, but only for the period necessary to comply with such requirement.
- 2.7 Supplier will keep detailed, accurate, and up-to-date records of its Processing, including: (a) the name and contact information for the Supplier and any representatives, Subprocessors and data protection officers; (b) the categories of Processing activities performed; (c) if Customer Personal Data is transferred to a third country, the details of that transfer including the safeguards taken; and (d) a description of the technical and organizational security measures implemented in respect of the Processing.
- 2.8 Supplier will help Customer with data protection impact assessments, privacy impact assessments, or other similar assessments. Supplier will notify Customer in advance of any proposed changes to the way Customer Personal Data is Processed, including proposed use of new technologies, so that Customer can assess whether a data protection impact assessment is needed.

3. **Details of Processing.** This Section 3 sets out certain information regarding Supplier's Processing of Customer Personal Data as required by article 28(3) of the GDPR, and possibly, equivalent requirements of other Data Protection Laws.
 - 3.1 **Subject Matter.** The subject matter of the Processing is the Customer Personal Data.
 - 3.2 **Duration of Processing.** The duration of the Processing of the Customer Personal Data is set forth in the Agreement and/or the relevant Statement of Work.
 - 3.3 **Nature and Purpose.** Supplier will Process Customer Personal Data as necessary to perform the Services pursuant to the Agreement, as further specified in the Statement of Work, if applicable, and as further instructed by Customer in accordance with this Addendum.
 - 3.4 **Type of Customer Personal Data.** The Customer Personal Data may include personal details, contact, account and financial information concerning the Data Subjects to the extent necessary to facilitate the Services as contemplated by the Agreement and the applicable Statements of Work.
 - 3.5 **Categories of Data Subjects.** The Data Subjects may include Customer's consumers, employees, suppliers, end users and agents.
4. **Subprocessing Of Customer Personal Data.** Supplier shall give Customer prior written notice of the appointment of any Subprocessor, including full details of the Processing to be undertaken by the Subprocessor. If, within sixty (60) days of receipt of that notice, Customer notifies Supplier in writing of any objections (on reasonable grounds) to the proposed appointment then Supplier shall not appoint (or disclose any Customer Personal Data to) that proposed Subprocessor until reasonable steps have been taken to address the objections raised by Customer and Customer has been provided with a reasonable written explanation of the steps taken. Supplier will engage a Subprocessor only pursuant to a written contract with the Subprocessor that obligates the Subprocessor to comply with this Addendum, including terms which offer at least the same level of protection for Customer Personal Data as those set out in this Addendum, the Agreement and the requirements of article 28(3) of the GDPR, if applicable. Supplier will remain liable for the actions of Subprocessors.
5. **Restricted Transfers.**
 - 5.1 **Standard Contractual Clauses.** Subject to Section 5.3, Customer (as "data exporter") and Supplier (as "data importer") hereby enter into the Standard Contractual Clauses (SCC) in respect of any Restricted Transfer from Customer to Supplier.
 - 5.2 **Effective Date of SCC.** The Standard Contractual Clauses shall come into effect under Section 5.1 upon the commencement of the relevant Restricted Transfer.
 - 5.3 **Limitation of SCC.** Section 5.1 shall not apply to a Restricted Transfer unless its effect, together with other reasonably practicable compliance steps (which, for the avoidance of doubt, do not include obtaining consents from Data Subjects), is to allow the relevant Restricted Transfer to take place without breach of applicable Data Protection Laws.
 - 5.4 **Representation.** Supplier warrants and represents that, before the commencement of any Restricted Transfer to a Subprocessor, Supplier's entry into the Standard Contractual

Clauses under Section 5.1, as agent for and on behalf of that Subprocessor, will have been duly and effectively authorized (or subsequently ratified) by that Subprocessor.

6. Data Security.

- 6.1 Supplier shall implement appropriate technical and organizational measures to protect Customer Personal Data from unauthorized access, acquisition, or disclosure, destruction, alteration, accidental loss, misuse, or damage that are no less rigorous than accepted industry practices, and all such safeguards, including the manner in which Customer Personal Data is created, collected, accessed, received, used, stored, processed, disposed of, and disclosed, will comply with applicable Data Protection Laws, as well as the terms and conditions of this Addendum. These safeguards shall include, but are not limited to: (a) pseudonymisation and encryption of Customer Personal Data; (b) the ability to maintain the on-going confidentiality, integrity, availability and resilience of Processing systems and services; (c) the ability to restore the availability and access to Customer Personal Data in a timely manner in the event of a physical or technical incident; and (d) a process for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures design to protect the security of Processing.
- 6.2 When assessing data security measures, Supplier will consider the risks presented by Processing Customer Personal Data, such as accidental or unlawful destruction, loss, alteration, unauthorized disclosure of or access to Customer Personal Data. Security measures will include: (a) limiting access of Customer Personal Data to authorized employees; (b) securing business facilities, data centers, paper files, servers, backup systems and computing equipment; (c) implementing network, application, database and platform security; (d) segregating Customer Personal Data from Supplier's other data; (e) conducting risk assessments, penetration testing and vulnerability scans; (f) implementing appropriate personnel security and integrity procedures and practices, such as background checks consistent with applicable law; and (g) providing appropriate privacy and data security training to employees.

7. Security Breach Procedures.

- 7.1 Supplier shall put in place an incident report strategy and shall notify Customer of a Security Breach without undue delay, but no later than twenty-four (24) hours after Supplier becomes aware of it. To the extent known, together with the Security Breach notification, Supplier shall provide to Customer (i) the details of the breach, including, but not limited to, the categories of Personal Data breached and the number of Data Subjects impacted; (ii) the kind of risk the breach is likely to present to the rights and privileges of Data Subjects; and (iii) any security measures, such as encryption and pseudonymisation measures, and any mitigating steps taken by Supplier.
- 7.2 Promptly following Supplier notification to Customer of a Security Breach, the Parties shall coordinate with each other to investigate the Security Breach. Supplier agrees to fully cooperate with Customer in Customer's handling of the matter, including, without limitation: (a) assisting with any investigation; (b) providing Customer with physical access to the facilities and operations affected; (c) facilitating interviews with Supplier's employees and others involved in the matter; and (d) making available all relevant records,

logs, files, data reporting, and other materials required to comply with applicable law, regulation, industry standards, or as otherwise required by Customer.

- 7.3 Supplier agrees: (a) to maintain and preserve all documents, records, and other data related to any Security Breach; and (b) in the event of any Security Breach, promptly use its best efforts to prevent a recurrence of any such Security Breach.
8. **Customer Audits.** Supplier will make available to MoneyGram all information necessary to demonstrate compliance with the obligations in this Addendum and the Data Protection Laws. Supplier will permit Customer and its third-party representatives to audit Supplier's compliance with its obligations under this Addendum and will give Customer and its third-party representatives all necessary assistance to conduct such audits.
9. **Indemnification.** In addition to the indemnification obligations set forth in Section 7 of the Agreement, Supplier will indemnify and hold harmless Customer for all claims and proceedings and all liability, loss, costs, fine and expenses (including reasonable legal fees) incurred by Customer arising from or in connection with (i) unauthorized Processing of Customer Personal Data by the Supplier, its employees or Subprocessors, (ii) Supplier's failure to comply with its obligations under this Addendum, or (iii) a Security Breach.
10. **Conflicts.** In the event of any conflict or inconsistency between this Addendum and the Standard Contractual Clauses, the Standard Contractual Clauses shall prevail. With regard to the subject matter of this Addendum, in the event of inconsistencies between the provisions of this Addendum and any other agreements between the Parties, including the Agreement and including (except where explicitly agreed otherwise in writing, signed on behalf of the Parties) agreements entered into or purported to be entered into after the date of this Addendum, the provisions of this Addendum shall prevail.



SCHEDULE A
TO THE DATA PROCESSING AND DATA PROTECTION ADDENDUM

STANDARD CONTRACTUAL CLAUSES

[These Standard Contractual Clauses are deemed to be amended from time to time, to the extent that they relate to a Restricted Transfer which is subject to the Data Protection Laws of a given country or territory, to reflect (to the extent possible without material uncertainty as to the result) any change (including any replacement) made in accordance with those Data Protection Laws (i) by the Commission to or of the equivalent contractual clauses approved by the Commission under EU Directive 95/46/EC or the GDPR (in the case of the Data Protection Laws of the European Union or a Member State); or (ii) by an equivalent competent authority to or of any equivalent contractual clauses approved by it or by another competent authority under another Data Protection Laws (otherwise).]

Standard Contractual Clauses (processors)

For the purposes of Article 26(2) of Directive 95/46/EC for the transfer of personal data to processors established in third countries which do not provide an adequate level of data protection. Customer and Supplier acknowledge that the transborder transfer of Personal Data shall be handled in accordance with the Standard Contractual Clauses for the Transfer of Personal Information to Processors established in Third Countries (2010/87/EU) (or equivalent model clauses in the UK, Switzerland, or EEA, as applicable) (“Model Contract Clauses”) and the Binding Corporate Rules (the “BCR-Processor”) of the Capgemini Group, which are available at <https://www.capgemini.com/resources/capgemini-binding-corporate-rules/> or can be sent to Client by electronic means on request. The parties agree that the BCR-Processor are fully integrated by reference into this DPA and, to the extent the BCR-Processor applies, are in lieu of Model Contract Clauses, if any, entered into by the parties. In case of contradiction or inconsistency between the terms of this DPA and the Model Contract Clauses (or BCR-Processor, as applicable), the Model Contract Clauses (or BCR-Processor, as applicable), shall prevail.

MoneyGram Payment Systems, Inc.

1550 Utica Avenue South, St. Louis Park, Minnesota, 55416, USA

.....
 (the data **exporter**)

And

Capgemini America, Inc.

79 Fifth Avenue, 3rd Floor, New York, NY

10003.....
 (the data **importer**)

each a “party”; together “the parties”,

HAVE AGREED on the following Contractual Clauses (the Clauses) in order to adduce adequate safeguards with respect to the protection of privacy and fundamental rights and freedoms of individuals for the transfer by the data exporter to the data importer of the personal data specified in **Appendix 1**.



Background

The data exporter has entered into a Business Services Master Agreement. (“**Master Agreement**”) dated August 20, 2020, with the data importer. Pursuant to the terms of the Master Agreement, it is contemplated that services provided by the data importer will involve the transfer of personal data to data importer. To maintain compliance with Directive 95/46/EC and applicable data protection law, the controller agrees to the provision of such services, including the processing of personal data incidental thereto, subject to the data importer’s execution of, and compliance with, the terms of these Clauses.

Clause 1

Definitions

For the purposes of the Clauses:

- (a) *'personal data', 'special categories of data', 'process/processing', 'controller', 'processor', 'data subject' and 'supervisory authority'* shall have the same meaning as in Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data; [If these Clauses are governed by a law which extends the protection of data protection laws to corporate persons, the words “except that, if these Clauses govern a transfer of data relating to identified or identifiable corporate (as well as natural) persons, the definition of "personal data" is expanded to include those data” are added.]
- (b) *'the data exporter'* means the controller who transfers the personal data;
- (c) *'the data importer'* means the processor who agrees to receive from the data exporter personal data intended for processing on his behalf after the transfer in accordance with his instructions and the terms of the Clauses and who is not subject to a third country's system ensuring adequate protection within the meaning of Article 25(1) of Directive 95/46/EC
- (d) *'the subprocessor'* means any processor engaged by the data importer or by any other subprocessor of the data importer who agrees to receive from the data importer or from any other subprocessor of the data importer personal data exclusively intended for processing activities to be carried out on behalf of the data exporter after the transfer in accordance with his instructions, the terms of the Clauses and the terms of the written subcontract;
- (e) *'the applicable data protection law'* means the legislation protecting the fundamental rights and freedoms of individuals and, in particular, their right to privacy with respect to the processing of personal data applicable to a data controller in the jurisdiction in which the data exporter is established;
- (f) *'technical and organisational security measures'* means those measures aimed at protecting personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.

Clause 2

Details of the transfer

The details of the transfer and in particular the special categories of personal data where applicable are specified in **Appendix 1** which forms an integral part of the Clauses.

*Clause 3****Third-party beneficiary clause***

1. The data subject can enforce against the data exporter this Clause, Clause 4(b) to (i), Clause 5(a) to (e), and (g) to (j), Clause 6(1) and (2), Clause 7, Clause 8(2), and Clauses 9 to 12 as third-party beneficiary.
2. The data subject can enforce against the data importer this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where the data exporter has factually disappeared or has ceased to exist in law unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law, as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity.
3. The data subject can enforce against the subprocessor this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity. Such third-party liability of the subprocessor shall be limited to its own processing operations under the Clauses.
4. The parties do not object to a data subject being represented by an association or other body if the data subject so expressly wishes and if permitted by national law.

*Clause 4****Obligations of the data exporter***

The data exporter agrees and warrants:

- (a) that the processing, including the transfer itself, of the personal data has been and will continue to be carried out in accordance with the relevant provisions of the applicable data protection law (and, where applicable, has been notified to the relevant authorities of the jurisdiction where the data exporter is established) and does not violate the relevant provisions of that jurisdiction;
- (b) that it has instructed and throughout the duration of the personal data processing services will instruct the data importer to process the personal data transferred only on the data exporter's behalf and in accordance with the applicable data protection law and the Clauses;
- (c) that the data importer will provide sufficient guarantees in respect of the technical and organisational security measures specified in **Appendix 2** to this contract;
- (d) that after assessment of the requirements of the applicable data protection law, the security measures are appropriate to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing, and that these measures maintain a level of security appropriate to the risks presented by the processing and the nature of the data to be protected having regard to the state of the art and the cost of their implementation;
- (e) that it will maintain compliance with the security measures;

- (f) that, if the transfer involves special categories of data, the data subject has been informed or will be informed before, or as soon as possible after, the transfer that its data could be transmitted to a third country not providing adequate protection within the meaning of Directive 95/46/EC;
- (g) to forward any notification received from the data importer or any subprocessor pursuant to Clause 5(b) and Clause 8(3) to the data protection supervisory authority if the data exporter decides to continue the transfer or to lift the suspension;
- (h) to make available to the data subjects upon request a copy of the Clauses, with the exception of **Appendix 2**, and a summary description of the security measures, as well as a copy of any contract for subprocessing services which has to be made in accordance with the Clauses, unless the Clauses or the contract contain commercial information, in which case it may remove such commercial information;
- (i) that, in the event of subprocessing, the processing activity is carried out in accordance with Clause 11 by a subprocessor providing at least the same level of protection for the personal data and the rights of data subject as the data importer under the Clauses; and
- (j) that it will maintain compliance with Clause 4(a) to (i).

Clause 5

Obligations of the data importer

The data importer agrees and warrants:

- (a) to process the personal data only on behalf of the data exporter and in compliance with its instructions and the Clauses; if it cannot provide such compliance for whatever reasons, it agrees to inform promptly the data exporter of its inability to comply, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;
- (b) that it has no reason to believe that the legislation applicable to it prevents it from fulfilling the instructions received from the data exporter and its obligations under the contract and that in the event of a change in this legislation which is likely to have a substantial adverse effect on the warranties and obligations provided by the Clauses, it will promptly notify the change to the data exporter as soon as it is aware, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;
- (c) that it has implemented the technical and organisational security measures specified in **Appendix 2** before processing the personal data transferred;
- (d) that it will promptly notify the data exporter about:
 - (i) any legally binding request for disclosure of the personal data by a law enforcement authority unless otherwise prohibited, such as a prohibition under criminal law to preserve the confidentiality of a law enforcement investigation,
 - (ii) any accidental or unauthorised access, and
 - (iii) any request received directly from the data subjects without responding to that request, unless it has been otherwise authorised to do so;
- (e) to deal promptly and properly with all inquiries from the data exporter relating to its processing of the personal data subject to the transfer and to abide by the advice of the supervisory authority with regard to the processing of the data transferred;
- (f) at the request of the data exporter to submit its data processing facilities for audit of the processing activities covered by the Clauses which shall be carried out by the data exporter or an inspection

body composed of independent members and in possession of the required professional qualifications bound by a duty of confidentiality, selected by the data exporter, where applicable, in agreement with the supervisory authority;

- (g) that, in the event of subprocessing, it has previously informed the data exporter and obtained its prior written consent;
- (h) that the processing services by the subprocessor will be carried out in accordance with Clause 11;
- (i) to send promptly a copy of any subprocessor agreement it concludes under the Clauses to the data exporter.

Clause 6

Liability

1. The parties agree that any data subject, who has suffered damage as a result of any breach of the obligations referred to in Clause 3 or in Clause 11 by any party or subprocessor is entitled to receive compensation from the data exporter for the damage suffered in accordance with Section 7 of the Agreement.
2. If a data subject is not able to bring a claim for compensation in accordance with paragraph 1 against the data exporter, arising out of a breach by the data importer or his subprocessor of any of their obligations referred to in Clause 3 or in Clause 11, because the data exporter has factually disappeared or ceased to exist in law or has become insolvent, the data importer agrees that the data subject may issue a claim against the data importer as if it were the data exporter, unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law, in which case the data subject can enforce its rights against such entity.

The data importer may not rely on a breach by a subprocessor of its obligations in order to avoid its own liabilities.

3. If a data subject is not able to bring a claim against the data exporter or the data importer referred to in paragraphs 1 and 2, arising out of a breach by the subprocessor of any of their obligations referred to in Clause 3 or in Clause 11 because both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, the subprocessor agrees that the data subject may issue a claim against the data subprocessor with regard to its own processing operations under the Clauses as if it were the data exporter or the data importer, unless any successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law, in which case the data subject can enforce its rights against such entity. The liability of the subprocessor shall be limited to its own processing operations under the Clauses.

Clause 7

Mediation and jurisdiction

1. The data importer agrees that if the data subject invokes against it third-party beneficiary rights and/or claims compensation for damages under the Clauses, the data importer will accept the decision of the data subject:
 - (a) to refer the dispute to mediation, by an independent person or, where applicable, by the supervisory authority;
 - (b) to refer the dispute to the courts in the jurisdiction in which the data exporter is established.

2. The parties agree that the choice made by the data subject will not prejudice its substantive or procedural rights to seek remedies in accordance with other provisions of national or international law.

Clause 8

Cooperation with supervisory authorities

1. The data exporter agrees to deposit a copy of this contract with the supervisory authority if it so requests or if such deposit is required under the applicable data protection law.
2. The parties agree that the supervisory authority has the right to conduct an audit of the data importer, and of any subprocessor, which has the same scope and is subject to the same conditions as would apply to an audit of the data exporter under the applicable data protection law.
3. The data importer shall promptly inform the data exporter about the existence of legislation applicable to it or any subprocessor preventing the conduct of an audit of the data importer, or any subprocessor, pursuant to paragraph 2. In such a case the data exporter shall be entitled to take the measures foreseen in Clause 5 (b).

Clause 9

Governing Law

The Clauses shall be governed by the law of the jurisdiction which the data exporter is established.

Clause 10

Variation of the contract

The parties undertake not to vary or modify the Clauses. This does not preclude the parties from adding clauses on business related issues where required as long as they do not contradict the Clause.

Clause 11

Subprocessing

1. The data importer shall not subcontract any of its processing operations performed on behalf of the data exporter under the Clauses without the prior written consent of the data exporter. Where the data importer subcontracts its obligations under the Clauses, with the consent of the data exporter, it shall do so only by way of a written agreement with the subprocessor which imposes the same obligations on the subprocessor as are imposed on the data importer under the Clauses. Where the subprocessor fails to fulfil its data protection obligations under such written agreement the data importer shall remain fully liable to the data exporter for the performance of the subprocessor's obligations under such agreement.
2. The prior written contract between the data importer and the subprocessor shall also provide for a third-party beneficiary clause as laid down in Clause 3 for cases where the data subject is not able to bring the claim for compensation referred to in paragraph 1 of Clause 6 against the data exporter or the data importer because they have factually disappeared or have ceased to exist in law or have become insolvent and no successor entity has assumed the entire legal obligations of

the data exporter or data importer by contract or by operation of law. Such third-party liability of the subprocessor shall be limited to its own processing operations under the Clauses.

3. The provisions relating to data protection aspects for subprocessing of the contract referred to in paragraph 1 shall be governed by the law of the jurisdiction in which the data exporter is established.
4. The data exporter shall keep a list of subprocessing agreements concluded under the Clauses and notified by the data importer pursuant to Clause 5 (j), which shall be updated at least once a year. The list shall be available to the data exporter's data protection supervisory authority.

Clause 12

Obligation after the termination of personal data processing services

1. The parties agree that on the termination of the provision of data processing services, the data importer and the subprocessor shall, at the choice of the data exporter, return all the personal data transferred and the copies thereof to the data exporter or shall destroy all the personal data and certify to the data exporter that it has done so, unless legislation imposed upon the data importer prevents it from returning or destroying all or part of the personal data transferred. In that case, the data importer warrants that it will guarantee the confidentiality of the personal data transferred and will not actively process the personal data transferred anymore.
2. The data importer and the subprocessor warrant that upon request of the data exporter and/or of the supervisory authority, it will submit its data processing facilities for an audit of the measures referred to in paragraph 1.

APPENDIX 1 TO THE STANDARD CONTRACTUAL CLAUSES

This Appendix forms part of the Clauses and must be completed and signed by the parties. The Member States may complete or specify, according to their national procedures, any additional necessary information to be contained in this Appendix.

Data exporter

The data exporter is MoneyGram Payment Systems, Inc., a Delaware corporation located at 1550 Utica Avenue South, St. Louis Park, Minnesota 55416, and operating in its capacity as a data exporter pursuant to the Master Agreement.

Data importer

The data importer is Capgemini America, Inc., located at 79 Fifth Avenue, 3rd Floor, New York, NY 10003 and acting as a data importer pursuant to the Master Agreement.

Data subjects

The personal data transferred concern the following categories of data subjects:

The personal data transferred concern data subjects who are citizens of one or more Member States, and who are protected by the European Communities Directive 95/46/EC or GDPR, and may include data exporter's consumers, employees, suppliers, end users and agents.

Categories of data

The personal data transferred concern the following categories of data:

The personal data may include personal details, contact, account and financial information concerning the data subjects to the extent necessary to facilitate the services as contemplated by the Master Agreement and any applicable Statements of Work entered into by and between the data exporter and the data importer.

Special categories of data (if appropriate)

The personal data transferred concern the following special categories of data:
none

Processing operations

The personal data transferred will be subject to the following basic processing activities:

The data importer will only process personal data as instructed by data exporter. Data exporter instructs data importer to only process personal data as reasonably necessary to provide the services as contemplated by the Master Agreement and any applicable Statement of Work entered into by and between the data exporter and the data importer.

APPENDIX 2 TO THE STANDARD CONTRACTUAL CLAUSES

This Appendix forms part of the Clauses and must be completed and signed by the parties.

Description of the technical and organisational security measures implemented by the data importer in accordance with Clauses 4(d) and 5(c):

Pursuant to the Master Agreement, between the data exporter and the data importer, the data importer is obliged to implement appropriate technical and organizational measures to protect the data subjects' personal data from unauthorized access, acquisition, or disclosure, destruction, alteration, accidental loss, misuse, or damage that are no less rigorous than accepted industry practices, and shall maintain that all such safeguards, including the manner in which personal data is created, collected, accessed, received, used, stored, processed, disposed of, and disclosed, comply with applicable data protection and privacy laws. These safeguards include, but are not limited to: (a) pseudonymisation and encryption of personal data; (b) the ability to maintain the on-going confidentiality, integrity, availability and resilience of processing systems and services; (c) the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident; and (d) a process for regularly testing, assessing and evaluating the effectiveness of technical and organizational measures to verify the security of processing.

Additionally, when assessing data security measures, the data importer will consider the risks presented by processing personal data, such as accidental or unlawful destruction, loss, alteration, unauthorized disclosure of or access to personal data. Security measures will include: (a) limiting access of personal data to authorized employees; (b) securing business facilities, data centers, paper files, servers, backup systems and computing equipment; (c) implementing network, application, database and platform security; (d) segregating data exporter's personal data from data importer's other data; (e) conducting risk assessments, penetration testing and vulnerability scans; (f) implementing appropriate personnel security and integrity procedures and practices, such as background checks consistent with applicable law; and (g) providing appropriate privacy and data security training to employees.

EXHIBIT E**ANTI-BRIBERY/ANTI-CORRUPTION REPRESENTATIONS, WARRANTIES AND COVENANTS**

- A. Supplier makes the following additional representations and warranties to Customer with the understanding that Customer is relying on them in entering into this Agreement, and further covenants that:
- (i) Supplier has not and will not offer, promise, make, or authorize the offering, promising, or making of any payment or transfer of anything of value (including cash or cash equivalents), directly or indirectly (1) to any person who is a Governmental Official (“**Government Official**”, as defined below in B or (2) to any other person or entity (“**Commercial Party**”, as defined in B) for the purpose of seeking improper action, inaction, influence, benefit, or undue advantage from such Government Official or Commercial Party in order to benefit Customer’s business;
 - (ii) except as disclosed to Customer, no Government Official has any legal or beneficial interest, direct or indirect, in Supplier or any payment to be made by Customer to Supplier under this Agreement;
 - (iii) except as disclosed to Customer, neither Supplier nor any shareholder, director, officer, employee who will be involved in the performance of services for Customer or agent of Supplier is a Government Official;
 - (iv) Supplier has adopted and will maintain during the term of this Agreement an anti-corruption policy (or Customer’s Anti-Bribery/Anti-Corruption Policy) which, at a minimum, prohibits the direct or indirect offer, authorization, or payment of money or anything of value to secure an undue advantage or improperly influence a Government Official or Commercial Party, and otherwise provides controls to assure compliance with the warranties contained in this Section and the keeping of accurate and complete books, records, and accounts of its activities hereunder;
 - (v) Supplier agrees that, if subsequent developments cause the representations and warranties made herein to no longer be accurate or complete, Supplier will immediately so advise Customer in writing and will cooperate with Customer to mitigate any risks that may arise from such subsequent development;
 - (vi) Supplier agrees that the Agreement is subject to immediate termination in the event that Supplier breaches the representations identified in this Section. Customer shall also have the right to withhold any payments that would otherwise be due to Supplier pending investigation of any allegations or information suggesting a possible breach, and to recover any monies paid to Supplier in the event it is determined such monies have been used in contravention of this **Exhibit E**; and
 - (vii) Customer shall have the right to inspect and audit the books, records, and accounts of Supplier relating to this Agreement for the purpose of verifying compliance with the terms of this **Exhibit E**, and to make copies (at its expense) of any such documents. Supplier shall cooperate with such inspection and audit, including making its personnel available to Customer to provide explanations of the books, records, and accounts of Supplier.
- B. For purposes of this **Exhibit E**,

- (i) a Government Official includes: (1) officers and employees of any government department, agency, commission, bureau, or authority, at any level of government (national, state or provincial, regional, or local), whether they are elected, career employees, or political appointees; (2) legislators and judges; (3) any persons acting in an official capacity on behalf of a government department, agency, or instrumentality; (4) officers and employees of entities that are owned or controlled by a government department, agency, or instrumentality; candidates for political office; (5) officers and employees of a political party, as well as the political party as an institution/entity; (6) officers and employees of any Public International Organization (an institution established by the national governments of sovereign countries, including but not limited to inter-governmental organizations); and (7) anyone else treated as a government official under any applicable local law or regulation; and
- (ii) a Commercial Party includes: any company, organization, or commercial entity whose personnel do not qualify as “**Government Officials**,” including any employee, agent, trustee, or fiduciary of such party.



EXHIBIT F**PRESCREENING CERTIFICATION**

This is to certify that the attached list of contractors was background checked for criminal, OFAC, and other required screenings no more than 30 days before each contractor first began performing work at any MoneyGram location. Your returned signature below will confirm that such background screenings have taken place and all listed contractors have been fully screened in compliance with legal requirements and the terms of the Agreement between Customer and Supplier.

Name of Supplier

Signed by

Date

EXHIBIT A-2

STATEMENT OF WORK

This Statement of Work (“**Statement of Work**” or “**SOW**”) adopts and incorporates by reference the terms and conditions of the Business Services Master Agreement (“**Master Agreement**”), which was entered into on September 3, 2020, between Capgemini America, Inc., a New Jersey corporation, having a principal place of business at 79 Fifth Avenue, 3rd Floor, New York, NY 10003 (“**Supplier**”) and MoneyGram Payment Systems, Inc., a Delaware corporation (“**Customer**” or “**MGI**”), as it may be amended from time to time. Customer and Supplier are jointly referred to as the “**Parties**”, and each, a “**Party**.” This SOW is effective beginning on September 3, 2023 (“**Effective Date**”) and will remain in effect until September 2, 2026 (“**Expiration Date**”), unless earlier terminated in accordance with the Master Agreement. Transactions performed under this SOW will be conducted in accordance with and be subject to the terms and conditions of this SOW, the Master Agreement, and any applicable purchase order (“**PO**”). This SOW is not a PO. Capitalized terms used but not defined in this Statement of Work shall have the meanings set out in the Master Agreement.

1. DEFINED TERMS

For purposes of this SOW, the following terms shall have the following meanings:

“**Agreement**”: Has the meaning specified in the first paragraph of this SOW.

“**Authorized User**”: Means MGI staff who are eligible to contact the Service Desk. This includes users that contact the Service Desk which are included in the ticketing system database, have access to and authorization to contact the Service Desk and/or use toolsets that interface with the Service Desk.

“**Business Day**”: Means 09:00 – 18:00 CDT, Monday – Friday, Business

“**Hours**”: Means 09:00 – 18:00 CDT, Monday – Friday, Commencement

“**Date**”: Has the meaning specified in Section 2.

“**Contact**”: Means any interaction between the Authorized Users and the Supplier Service Desk personnel (e.g., via phone, MGI Self Service Portal, email)

“**Contact Channel**”: Means the contact method that an Authorized User employs to contact the Service Desk

“**Deliverable**”: Means the tangible materials developed or to be developed by Supplier specifically for Customer hereunder and required to be delivered to Customer by virtue of their description or specification as a Deliverable under this Statement of Work or future documentation.

“**Early Life Support Period**”: Means the period of three months after the Commencement Date.

“**Effective Date**”: Has the meaning specified in the first paragraph of this SOW.

“**Exhibits**”: Means any schedule, exhibit, attachment, agreement or other document either (i) attached to this SOW, (ii) attached to an addendum, or (iii) executed by the parties at any time hereafter if such document states that it is a schedule, exhibit or attachment to this SOW or the Agreement.

“**Incident**”: Means an unplanned interruption to an IT Service or reduction in the quality of an IT service. Failure of a configuration item that has not yet affected service is also an incident.

“**Knowledge Article**”: Means a document within the MGI ticketing tool that provides instructions for the Service Desk to resolve Incidents and Service Requests.

“**Knowledge Base**”: Means a database within the ticketing tool/service knowledge management system that includes Knowledge Articles.

"Knowledge Database": Same as Knowledge Base.

"Knowledge Object": Means a subset of Knowledge articles specific to a particular system/ application

"Knowledge Management": Means the process responsible for gathering, analyzing, storing, and sharing knowledge and information related to delivery of Services.

"Relief Event": Means (i) a failure by MGI or any MGI third party to comply with its obligations or (ii) any failure to perform by Supplier that arises from any negligent or willful act or omission by MGI or any MGI third party or (iii) a force majeure event.

"Problem": Means the underlying cause of one or more incidents.

"Service Desk": Means the Supplier's people, facilities, people and infrastructure to provide the Services defined in this SOW.

"Service Desk Services": Means the Services as defined below in Sections 4 and 5.

"Service Level" together with "Service Level Agreement" or "SLA": Means a quantitative level of performance for certain specified Services. With respect to each Service that has an associated Service Level, Supplier shall provide such Service throughout the Term in a manner that meets or exceeds the associated Service Level Target (as defined in individually with each Service Level).

"Service Level Commencement Date": Means the date upon which Supplier is required to meet the Service Levels applicable to Supplier.

"Service Level Measure": Means the method for quantitatively calculating Supplier's actual performance. The results of these calculations are compared with Service Levels to evaluate Supplier's compliance with the Service Levels.

"Service Request": Means an Authorized User request for information or advice, or for a standard change (a pre-approved change that is low risk, relatively common and follows a procedure) or for access to an IT service.

"Services": Means both the Transition Services and Service Desk Services, as defined below in Sections 4 and 5.

"Statement of Work" or "SOW": Has the meaning specified in the first paragraph of this SOW. Term: Means the term of this Statement of Work.

"Ticket": Means an entry (e.g., Service Request or Incident) in the ticketing tool.

"Transition" or "Transition Services": Means process or activities to acquire knowledge of the existing MGI environment and to establish Supplier Service Desk environment prior to Commencement Date.

"MGI Engagement Manager": Means the individual who is the primary MGI interface for issues related to the day-to-day performance of the Services.

2. TERM

2.1 Initial Term

Services under this Statement of Work shall begin on September 3, 2023 (the "Commencement Date") and continue for a period of thirty-six (36) months (the "Term").

2.2 Renewal Term

The Parties may agree to extend the initial Term of this SOW provided that any such extension must be agreed upon by the Parties in writing no later than ninety (90) calendar days before expiration of the Initial Term or any subsequent renewal Term.

2.3 Early Termination

Customer shall be entitled to terminate this SOW for convenience without cause upon no less than ninety (90) days' prior written notice to Supplier.

3. SERVICE COMPONENTS

The Services are comprised ongoing delivery and running of Service Desk Services.

4. SCOPE OF WORK

Service Desk Services Overview

This Section provides information on Service Desk Services provided by the Supplier for MGI. The Services will be delivered as Managed Services out of India.

The Supplier will provide the activities and functions listed below:

- a. Contact handling
- b. Incident Coordination
- c. Service Request fulfillment
- d. Standard Service Desk performance reporting
- e. User Satisfaction Survey

5. SPECIFICATION

5.1 Service Desk Services

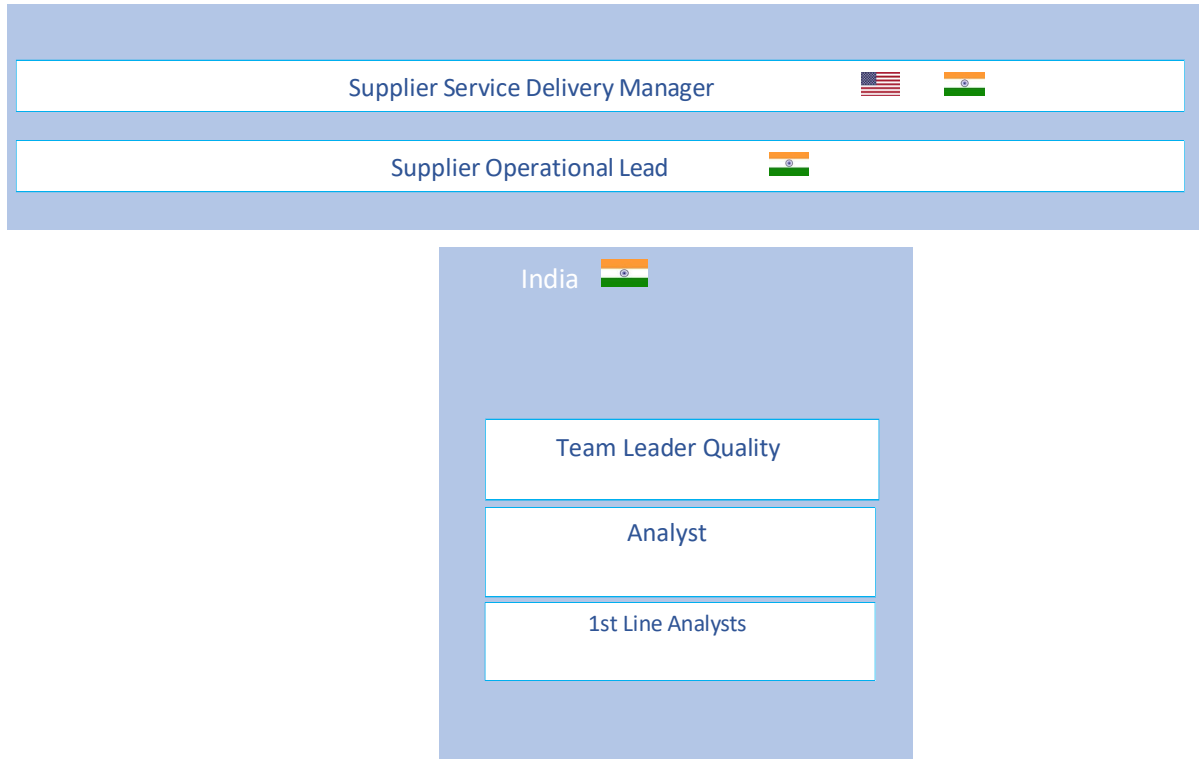
The Service Desk is a Single Point of Contact (SPOC) for Authorized Users and is responsible for recording, responding to, resolving, and reporting information technology-related Incidents and Service Requests. The list of applications and key technologies with corresponding level of support will be collected during Transition to establish a baseline of Contact types to be supported by Supplier.

- a) The Service Desk shall handle and record all Authorized User-reported information technology-related issues in the form of Incidents and Service Requests.
- b) The Authorized Users may only contact Service Desk via telephone, MGI Authorized User Portal, and email.
- c) Supplier shall provide access to the Service Desk Interactive Voice Response ("IVR") system for calls dialed by the Authorized User using a local geographical telephone numbers provided by MGI; Supplier is responsible for providing only phone number in US (Genesys) where all end users' calls shall be directed by MGI. MGI is responsible for provision of local Service Desk telephone numbers.
- d) Supplier and MGI shall continuously educate, through mutually agreed timing and means, Authorized Users on the use of the Service Desk.
- e) Supplier shall provide and maintain instructions for Authorized Users to access the Service Desk. The instructions will be made available to Authorized Users via various media, agreed and approved by MGI and Supplier.
- f) Communication with the Authorized User to the Service Desk, all activities, recordkeeping, reports, or other communications with MGI shall be performed by Supplier using the English language.
- g) Supplier shall log all Tickets in MGI's ticketing system; all licenses and access to the ticketing system and tools are to be provided by MGI. Supplier shall update the Knowledge Database with Knowledge Articles created during the Transition Services and received from MGI, other third parties, and the Supplier's resolver groups.
- h) The target Supplier operating model for the Services is depicted below:

The role of Supplier Service Delivery Manager shall be located either in the United States or India.

The roles of Supplier : Operational Lead, Team Leader, Quality Analyst, and 1st Line Analysts shall all be based in India during the Term of the Agreement.

Statement of Work for Service Desk Managed Services



5.1.1 Service Desk – Roles and Responsibilities

Role	Location	Responsibility
Service Delivery Manager	<ul style="list-style-type: none"> US or India 	<ul style="list-style-type: none"> Manages overall service delivery and is the main contact for MGI management Takes responsibility for end-to-end in-scope service delivery and quality of Services as well as fulfillment of the contractual SLA
Operations Lead	<ul style="list-style-type: none"> Supplier Service Delivery Center 	<ul style="list-style-type: none"> Manage Services effectively. Monitoring that Capgemini and MGI work according to procedures. Day-to-day interface between the Service Desk and MGI's Engagement Manager Provide appropriately skilled and trained resources and ensure that they are working in accordance with the agreed procedures

Role	Location	Responsibility
Team Leader	<ul style="list-style-type: none"> Supplier Delivery Center 	<ul style="list-style-type: none"> Leads the Supplier team to achieve levels of service that meet the SLA. Develop, manage, and maintain effective working relationships with all Authorized Users. Provide a well-structured and professional working environment. Effectively manage and motivate the Supplier team. Responsible for monitoring performance against the SLA. Allocate work to Supplier team(s) and motivate Supplier team(s) Manage Supplier team issues and risks
1st Line Analysts	<ul style="list-style-type: none"> Supplier Service Delivery Center 	<ul style="list-style-type: none"> Answer all contacts efficiently in a professional and courteous manner in English Address Service Requests and Incidents or escalate to resolving teams outside of Service Desk Record all Supplier-performed steps to address an Incident or Service Request Call backs, troubleshooting, procedural follow ups as agreed to address Incidents and Service Requests in scope Handle Incidents and Service Requests according to MGI's assigned priorities Search and update work procedures according to the Knowledge Management Process in the Knowledge Base
		<ul style="list-style-type: none"> Promote standard Supplier Request and Incident Management Process across all support tiers and apply business and technical knowledge effectively so that service levels are addressed Help reduce the impact of reported Incidents on MGI's business Help to facilitate working relationships across service lines (e.g., Capgemini, MGI, third party, and partner contacts), to the extent he or she is able to do so. Support the Knowledge Management process by flagging material for reuse (e.g., feed information via Knowledge Managers into the Knowledge Base).
		<ul style="list-style-type: none"> Manage the Knowledge Base Procedure review: Review procedures - contact the resolver teams, subject matter specialist ("SMS"), and procedure owner in order to analyze

Role	Location	Responsibility
Quality Analyst		<p>the procedures and update or archive the obsolete articles</p> <ul style="list-style-type: none"> Reporting: Generate regular and ad hoc reports from the Knowledge Base on the status of solutions accordingly to leading practices and agreed requirements (this is a monthly task) Management of the Knowledge Management Process: Prepare, review and update the Knowledge Management work instructions, solution templates and process document accordingly to Knowledge Management leading practices and agreed requirements (upon request –a bimonthly task) Supplier Team training coordination Continuous expansion of Knowledge Articles Ticket templates: recommend the creation, updating, and archiving of ticket templates within the MGI ticketing system once validation from the procedure owner, SMS, or resolving team is received.
	<ul style="list-style-type: none"> Supplier Service Delivery Centers 	<ul style="list-style-type: none"> Oversee the quality of service provided to MGI to enable Service Levels to be met Support 1st Line Analyst with quality-related issues Manage quality check process Reporting: Prepare quality performance reports on monthly basis and prepare improvement plans for the whole team and for individual, if necessary.

5.1.2 Service Desk - Contact Handling and Incident Coordination

The Service Desk shall provide contact handling that will consist of:

- Logging the Contact and opening an entry Ticket in the ticketing tool, updating the Incident ticket with all relevant information relating to each Incident, including the description of the Incident and the Authorized User details.
- Making an initial determination, including prioritization (which includes setting the priority of Incidents) and categorization of tickets according to work instructions in the Knowledge Base;
- Supplier shall determine the assignment of tickets to Level 2 or 3 resolver groups of Incidents that cannot be resolved at Level 1 on the basis of allocation rules predefined by MGI. The determination will be based on the up-to-date work instructions available in the Knowledge Base.
- Where technically possible, connecting to the Authorized User's personal computer via the remote connectivity tool to perform the necessary action utilizing MGI's remote connectivity tool Bomgar.
- Providing or coordinating the resolution if a fix is known and recorded in the Knowledge Database.

- f) Where the issue cannot be resolved by the Service Desk, the Service Desk agents will assign the Ticket to the appropriate MGI/Third-Party provider Level 2 or Level 3 resolver group based on Knowledge Articles available in the Knowledge Database.
- g) Supplier shall link multiple Incidents pertaining to a master Incident or to Problem record.

5.1.3 Service Desk –Service Request Fulfilment

Service Request fulfilment is the process of handling standard Service Requests throughout their lifecycle.

Supplier shall manage the process of communication with the Authorized Users in respect to Service Request status and closure, subject to approval by MGI.

- a) Supplier shall receive all Service Request-related interactions from any Authorized Users (via the agreed communications channels) and identify and capture the nature and information of the interaction, or the Authorized User is enabled to send the request directly to the resolving team.
- b) Supplier shall support Authorized Users who submit Service Requests, requests for guidance, or advice via phone.
- c) Supplier shall utilize and update the ticketing tool with all relevant information relating to each Service Request, including the description of the Service Request and the Authorized User details.
- d) Supplier shall link multiple contacts pertaining to the same Service Request record to the associated Service Request record.
- e) Supplier shall, if the Service Request does not apply to a Service Request model or cannot be fulfilled by using a standard change, inform the Authorized User that the request cannot be fulfilled and reject the Service Request. If required, the Supplier shall escalate to MGI the Service Request that does not conform with the criteria and policies specified by MGI.
- f) Supplier shall identify the Service Request category as set out in the agreed categorization scheme.
- g) Supplier shall prioritize the Service Request according to agreed work instructions in the Knowledge Base.
- h) Supplier shall determine the assignment to other resolver groups of Service Requests that cannot be fulfilled on the basis of allocation rules predefined by MGI and update the ticketing tool.
- i) Supplier shall escalate conflicts or issues where MGI or its third parties are responsible for the Service Request resolution.
- j) Supplier shall only perform the resolution if fix is known and recorded in the Knowledge Base.
- k) All Service Requests are considered pre-approved and Supplier Service Desk will not be responsible for approval gathering.

5.1.4 Service Desk – Languages and Hours of Support

Supplier shall provide support to MGI's Authorized Users in the following :

- Language: English Only.
- Support Hours: Monday to Friday 24 Hours (24X5) including MGI and India holidays

BackOffice roles such as: Team Leader and Quality Analyst will be available during Monday to Friday for 9 hours per day. The processes to be delivered as per Capgemini best practice and standard processes.

5.1.5 Service Desk Locations

Supplier shall provide support to MGI's Authorized Users from the following Delivery locations:
India for the English language.

5.1.6 Service Desk - Reporting

Supplier's responsibilities regarding reporting will consist of:

- a) Monthly tracking and reporting any backlog of unresolved Incidents or Service Requests.
- b) Performance against SLAs.
- c) Conduct bi-weekly & monthly meetings with MGI to review the deck, during which, we can give recommendations for improvements such as: service interaction, volume reduction or increases, productivity, training for Authorized Users, trends in top issues/requests received and/or service offering enhancements.

The list of standard reports to be mutually agreed upon during Transition, which may be amended by mutual agreement. Sample list of reports are as follows:

- 1. Daily dashboard
- 2. Bi-Weekly report
- 3. Monthly report

Capgemini will share Telephony statistics via Genesys Dashboards (shared daily) which will include data such as : number of calls received, number of calls picked up, and number of calls abandoned.

Service Desk - User Satisfaction Survey

MGI shall provide automated Authorized User satisfaction surveys which will be as follows:

- a) In an effort to seek feedback from Authorized Users who have contacted the Service Desk about the handling of Contacts by the Service Desk, the ticketing tool will trigger an automatic user survey based on an agreed standard set of four questions; At times, some user feedbacks are excluded from consideration based on client's approval.

5.1.7 Service Desk - Service Improvement

- a) The Supplier will provide continual improvement as part of its Services using MGI supplied tools and Capgemini's processes. Capgemini will investigate incidents and service request trends to suggest and mutually drive improvements for the processes.
- b) Capgemini has a training plan for any new resource onboarding the team. The same plan will be used for future additions in the team as well.
- c) Capgemini will have periodic reviews with MGI to review documented feedback on the Services provided and to create mutually agreeable improvement plans for the Services. The improvement plan can span across resources, services, skillset and technology.

5.1.8 Service Desk – Infrastructure Setup**5.1.8.1 MGI shall establish and maintain the VDI infrastructure for Service Desk agents to connect from Supplier Network**

- a) Access the MGI Intranet via logging in to Supplier network via VDI
- b) Use MGI purchased and supplied VPN tokens to access the required service desk tools
- c) Access to MGI ITSM (ServiceNow), Password reset, Bomgar.

5.1.8.2 Telephony Solution:

- a) Supplier uses a mutualized contact center solution, Genesys platform which is a cloud- based telephony solution. Genesys will be managed by Supplier. It will collect calls on Supplier's platform from a local telephone number in US provided by Supplier and connect via IVR which distributes calls to Supplier delivery center in India.
- b) To contact Supplier Service Desk, MGI Authorized Users will have to call the local numbers provided by MGI in each country, and their calls will be connected to Supplier delivery center via the Genesys cloud. MGI will re-direct the local telephone numbers to technical number in US provided by Capgemini.

It is expected that the telephony solution is aligned with MGI's security requirements. If not, then a detailed solution shall be mutually agreed upon and priced.

5.1.9 Service Desk - Governance

The proposed governance model will be separated into three tiers: Executive Steering Committee, Management Committee, and Operational Committee:

- The **Executive Steering Committee** will be responsible for setting the overall direction for the Services, developing the business relationship between the organizations, and aligning the Project Goals/Objectives with the Business Goals/Objectives
- The **Management and Strategy Committee** will be responsible for participating in the development and implementation of the objectives/goals and providing management of the Transfer/Transition/Transformation, ongoing Service and effective utilization of resources and technology platform(s)
- The **Operational Committee** will be responsible for the day-to-day operation and management of service delivery.

The governance structure will be updated to reflect agreed roles, titles, and names, and the governance structure may be modified during the Term as appropriate.

5.1.10 Service Desk – MGI Responsibilities and Service Desk assumptions

The performance of services, schedule, resources, and service levels provided in this SOW are based upon the following volumes and assumptions. Should these assumptions change, the fees, expenses, and schedule associated with this project may need to be adjusted.

MGI Responsibilities and Service Desk assumptions:

1. MGI will put in place the commercial arrangements required with their third-party suppliers to ensure that the third-party suppliers will work collaboratively and provide data/information and training as required by the Supplier in performance of its duties under this SOW. MGI will provide and maintain the escalation/assignment matrix and act as an escalation point for the cross-supplier issues.
2. MGI will ensure the Supplier has full access to the necessary data, as well as MGI and third-party SMEs and systems according to the timeline in performance of its duties under this SOW.
3. MGI will ensure that Supplier has access to knowledge regarding business processes, key activities, key performance indicators, training on tools, etc. needed to assist Supplier personnel in delivering the Services.
4. MGI will ensure that the workflow relating to Requests logged from the Self-Service Portal by Authorized Users have been duly authorized by MGI before its receipt by the Service Desk.
5. MGI will establish and provide roles to interface with Supplier governance structure described in Section 5.1. MGI will engage with Supplier and third-party suppliers in discussions around Service Desk improvement areas and shall support the Supplier by acting as an escalation for Service Desk Services with third party suppliers.
6. MGI shall include Supplier into the MGI change management process for those changes that will impact the Services, MGI shall give Supplier reasonable notice ahead of any anticipated major or significant changes to MGI's IT Environment that would affect the Service Desk Services.
7. Provide VDI with dual factor authentication for Service Desk agents.

8. MGI shall configure the MGI ticketing tool to enable the Service Desk to log tickets and perform other tasks efficiently; this includes but is not limited to: Knowledge, Incident, Service Request and MGI Survey modules configured, list of Authorized Users details, templates, automated email notifications, configuration of the defined Service Levels, and the ability to perform automated reporting on the contracted SLAs as well as automated dashboards for operational reporting purposes.
9. MGI will provide Service Desk with all relevant accesses and permissions to the tools and systems to enable to perform Services under this SOW. This includes licenses and access to: MGI ITSM ticketing tool (Service Now), Remote Connectivity Bomgar tool, Password Reset Console, etc.
10. MGI is responsible for providing and management of the inbound telephone numbers for the Authorized users. The numbers will be directed to the Capgemini telephone number in US. All costs of this re-direction as well as inbound telephony costs to US number will remain on the customer side.
11. Service Desk has been designed to support the following volumes:
 - a. Monthly volumes: 2,500 (400 calls and 2,100 Self-service portal tickets)
 - b. End user count: 2,277 (corporate user)
 - c. Average handling times per contact:
 1. Call 9.5 minutes
 2. Self service ticket - 10 minutes

In the event any actual volumes would exceed or reduce the designed support volumes by ten percent (+10% or -10%), the Parties shall actively and in good faith negotiate and implement an equitable adjustment of the rates and charges via a change order.
12. SD resolution to be based on pre-defined Fixable Issues list. Service Desk is designed to perform 40% resolution out of total ticket volume (90% out of pre-defined Fixables).
13. Assumed all knowledge to be gathered from MGI over remote sessions. As originally it was planned to have on-site visits at incumbent in India to gather all necessary knowledge it is expected that Customer will ensure the availability of the relevant resources as per Capgemini proposed knowledge gathering/ training agenda. Assumed MGI to be cooperative and share the relevant knowledge.
14. It is assumed that the ticketing tool will be configured in a way to enable the Service Desk to log the tickets efficiently and to perform automated reporting from the contracted SLAs.
15. Customer is responsible for configuration of reporting module within the ITSM tool to enable efficient and accurate reporting. SLAs are applicable only if reporting module is configured and proper accesses are granted to Capgemini.
16. Service Desk to sign off the SLAs implementation in ticketing tool.
17. Assumed Capgemini does not have to create any knowledge and upload it to Service Now, it is expected the knowledge is available in Service Now.
18. All knowledge related to Service Desk activities is well-documented and available via Ticketing tool, knowledge articles include all relevant guidance in reference to the tools which may be used by Service Desk as well as instructions related to support activities and resolution.

5.1.11 Service Desk – Exclusions

The following elements have been excluded from Capgemini's offer:

1. Inbound telephone numbers
2. Dedicated network for Service Desk agents network connectivity
3. Provisioning of VDI for Capgemini Service Desk agents for MGI network access
4. Service Desk tools (remote connectivity tool, ITSM ticketing tools, password reset tool, etc.)
5. Remote 2nd Line Team

6. PERSONNEL

The following roles are the principal contract for the Services from each Party.

1. Supplier Personnel: Supplier Services Delivery Executive

2. Customer Personnel: Customer Engagement Manager

7. PRICING

Supplier will invoice for the Monthly Services Fees each Month at the fees and rates set forth in the tables below. The Monthly Services Fees will be invoiced in the USA in \$USD and are exclusive of taxes and other expenses.

Monthly base fees will be invoiced upon the Effective Date, unless otherwise set forth below.

Monthly Base Fees

Services	Year 1	Year 2	Year 3
Monthly Base Level 1/Level 1.5 Support	\$25,211	\$24,323	\$23,303
Twelve (12) Month Total	\$302,532	\$291,323	\$279,303
SOW Total	\$874,044		

7.1 Payment

Customer will pay Supplier's invoices within sixty (60) days of the date of each invoice.

8. SERVICE LEVELS MANAGEMENT**8.1 General**

The Service Levels sets out both the nature and the quality of the Services provided, and the obligations placed on both parties related to the performance of the Services.

8.2 Actions and Escalations

For non-critical (no impacts to Service Levels) issues, each party's operations will utilize the Customer's ITSM tool to report incidents. Supplier will undertake actions to improve any individual Service Level that receives a score Service Level Missed below. These actions are described in Table A below. Further, escalation procedures, as set forth in Table B below, will provide management attention to incident areas consistent with the impact of the incident.

Table A – Action Matrix

The performance of each Service Level will be reviewed Monthly. Corresponding actions that will be taken are set out below.

Individual Service Level Score	Improvement Actions to be Taken by Supplier
Service Level Met	For any Service Level which scores " Service Level Met " during the Measurement Period, no action other than the periodic Service Level review is required.
Service Level Missed	For any Service Level which scores " Service Level Missed ", during the Measurement Period, Supplier Service Delivery Executive will develop a solution to the problem, will notify the Customer Engagement Manager of the effort, and will obtain Customer agreement to the solution implementation.

Escalation Procedures

Escalation procedures have been developed so that the appropriate management attention is devoted to outstanding incidents consistent with their impact. Each outstanding incident will be categorized with a priority level and assigned the appropriate level of resources consistent with its impact. This escalation procedure increases the level of resources as necessary to resolve incidents effectively. Supplier will clarify the incident situation and communicate action plans to Customer within a time frame appropriate to the severity of the pending incident. Supplier will take a pro-active approach to notifying both Supplier management and Customer management according to the below.

Table B – Escalation Criteria and Notification

Priority 1 Escalation Criteria	Person Notified
Any Priority 1 incident outstanding past defined incident resolution time.	Supplier will notify based on the escalation matrix.
Any Priority 1 incident outstanding for two (2) hours past defined incident resolution time.	Supplier will notify the Customer Engagement Manager and Supplier Services Delivery Executive.
Priority 2 Escalation Criteria	Person Notified
Any Priority 2 incident outstanding past defined incident resolution time.	Supplier will notify the designated Customer team leader.
Any Priority 2 incident outstanding for two (2) hours past defined incident resolution time.	Supplier will notify the Customer Engagement Manager and Supplier Services Delivery Executive.
Priority 3 Escalation Criteria	Person Notified
Any Priority 3 incident outstanding past defined incident resolution time.	Supplier will discuss in weekly status meeting.
Any Priority 3 incident outstanding for four (4) hours past defined incident resolution time.	Supplier will notify the designated Customer team leader and discuss in weekly status meeting.

The table below defines the priorities for incidents.

Priority	Definition
Priority 1 ("P1")	Priority 1 Critical Business Impact – System down or immediate work stoppage of a critical business service that threatens current and future productivity.
Priority 2 ("P2")	Priority 2 Significant Business Impact – incident where system or business service is proceeding but in a seriously impaired or in a restricted fashion and no acceptable workaround is possible.
Priority 3 ("P3")	Priority 3 Some Business Impact – incident for which the impact is an inconvenience, which may require a workaround to restore functionality and productivity is not seriously impaired.
Priority 4 ("P4")	All other incidents or requests.

8.3 Service Levels

The Service Levels describe the key areas of measurement used for demonstrating compliance with the provision of Services described hereunder.

Each Service Level is described using the following components.

"Service Level Target" is the Service Level performance target.

"Service Level Description" is the description of the Service being measured.

“Measurement Tool” is the tool used to collect the Service Level data and calculate the Service Level measurement.

“Service Level Calculation” is the calculation for how the Service Level Target will be calculated.

“Measurement Period” is the periodic basis for which performance reports for the Service Level will be delivered.

Supplier will monitor, measure, calculate and report all Service Levels. Data will be collected Monthly and will be reported within ten (10) Business Days after the end of a Month.

Detailed reporting as well as measurements will be agreed mutually during Transition. Supplier will be granted sufficient accesses to test the reporting during Transition and sign off on the SLA measurements.

8.4 Service Level Matrix

The Service Levels applicable to the Services are set forth in the following table:

Service Level	Service Level Description	Service Level Target	Weighting Percentage	Service Level Measurement	Service Level Commencement
SL_SD_1.2	Grade of Service for telephone calls	80% of phone calls answered within 30 seconds	10%	The total number of telephone calls answered by the Service Desk during a month. Measured as the time from when the user selects to speak to an agent from the automated menu to the end of the target time period (30 seconds) divided by (the total number of telephone calls offered to the Service Desk in that month minus any abandoned calls) * 100	SOW Effective Date
SL_SD_1.3	Grade of Service for self-service portal tickets	80% within 4 Business Hours	20%	Calculation: Number of Tickets where Reaction time is <= 4 Business Hours. Reaction time is measured as time from which a portal ticket is received in ITSM to the time it will be changed/modified in to an Incident or a Service Request and is Categorized and assigned to the proper resolver team) / All portal tickets (Excluding all tickets bypassing the Service Desk) received in SNOW * 100	SOW Effective Date
Service Level	Service Level Description	Service Level Target	Weighting Percentage	Service Level Measurement	Service Level Commencement

SL_SD_1.5	P1 Ticket Routing Limited to Supplier in scope tickets	90% within 30 minutes	10%	% of P1 incidents logged via voice channel per into Service Desk in a 3 month period and routed within target P1 description is per MGI severity and priority guidelines. Subject to Low Volume Metrics. Minimum. Minimum volume for this Service Level is 3 within a quarter	SOW Effective Date
SL_SD_1.5	P2 Ticket Routing Limited to Supplier in scope tickets	90% within 30 minutes	10%	% of P2 incidents logged via voice channel into Service Desk in a 3 month period and routed within target P2 description is per MGI severity and priority guidelines. Subject to Low Volume Metrics. Minimum volume for this Service Level is 3 within a quarter	SOW Effective Date
SL_SD_1.7	P3 Fix (Incident/Request Response/Fix) Limited to Supplier in scope tickets	90% next Business Day	20%	% of P3 incidents in a month fixed within target P3 description is per MGI severity and priority guidelines. Urgent UAR User Access Request (Request)	SOW Effective Date
SL_SD_1.8	P4 Fix (Incident/Request Response/Fix) Limited to Supplier in scope tickets	90% in 3 Business Days	10%	% of P4 incidents in a month fixed within target P4 description is per MGI severity and priority guidelines.	SOW Effective Date
SL_SD_1.9	Resolution of Service Requests within prescribed time. Limited to Supplier in scope tickets.	90% of Service Requests resolved within 2 business days where no MGI intervention is required.	20%	% of Service Requests in a month resolved within target.	SOW Effective Date

Genesys KPIs:

Restoration Time for Genesys P1 (Critical Incidents) – 95% in 4hrs.

The Restoration is the duration elapsed between:

- The record in the Genesys ITSM tool following a submission by the authorized personnel of the

Customer to the Genesys Service Desk via authorized contact channel.

- Service is restored to an operational level (Including workaround solution with priority decrease)

Measurement: ORT1 (Genesys Restore Time P1)

Calculate the duration of each incident excluding the stand by (On hold/awaiting for customer feedback) period:

Starting point = T1 (is the time when the incident ticket is opened in the Genesys ITSM tool and assigned to the proper skills)

End point = T3 (means the time the incident is resolved. Ticket is closed by Genesys and the customer is informed of the end of the incident.)

(Total ticket count – Tickets with breached restore Time)

Calculation = $\frac{\text{Total ticket count} - \text{Tickets with breached restore Time}}{\text{Total ticket count}} * 100$

Genesys : Cloud Availability: 99.9 %

Description:

Core of the service represents 99.9% of calls requesting an agent (through IVR) reaches agent.

Provider guarantees this overall availability of the Service including:

- ☐ Availability of the phone numbers is excluded as it is MGI to provide inbound telephone numbers.
- ☐ The availability is applicable only for the infrastructure elements managed by Genesys
- ☐ Call collected on US local number and transferred to an agent.
- ☐ TOIP
- ☐ IVR

8.5 Effective Date for Service Levels

Supplier Service Levels attainment obligations shall be tracked upon the Services Commencement Date through the Term of this SOW.

8.6 Single Point of Contact

Regardless of whether any failure by Supplier to meet a Service Level is attributable to Supplier or an excused performance problem as described in Section 8.9 hereunder, Supplier shall provide a single point of contact to address resolution of such failure and shall act promptly to address the problem causing the failure. Unless otherwise agreed to by Customer, the Supplier Service Delivery Executive, or his/her designee, shall be the Supplier single point of contact.

8.7 Low Volumes

For Service Level Measurements that are based on low volumes (e.g., a Service Levels Measurement where the number of measured data points is so low that a single failure could result in a failure by Capgemini to meet or achieve the applicable Service Level Target) ("Low Volume Measurement Window"), the Calculation for the Service Level Measurement for the applicable Service Level will be adjusted using the pre-defined formula as set forth below, based on the actual volume such that a single failure does not result in a Service Level failure.

In each Low Volume Measurement Window for any Service Level Measurement that Capgemini would be precluded from addressing due to an insufficient number of measured tasks, the Service Level Target shall be adjusted to equal the quotient (expressed as a percentage) determined by dividing (i) the total number of measured tasks in such Low Volume Measurement Window minus one (1), by (ii) the total number of measured tasks in such Low Volume Measurement Window.

For example, if the Service Level Target is 90% or greater, there would need to be at least 10 measured tasks in order to allow Capgemini to meet the Service Level in a Measurement Period in which it has one (1) failure to meet, achieve or perform the measured tasks (e.g., 1 miss in 10 = 90% success rate). Thus, if the Service Level Target is 90%, and if the total number of measured tasks for such Service Level in a Low Volume Measurement Window is 8, then the Service Level Target in such Low Volume Measurement Window shall be 87.5% (the quotient, expressed as a percentage, determined by dividing (x) 7 (e.g., 8 minus 1) by (y) 8).

- 1) Service Level Failures

If Supplier fails to meet a Service Level, Supplier shall provide Customer with a written plan for improving Supplier's performance within fifteen (15) calendar days of the failure to meet such Service Level. A Service Level failure shall consist of the actual failure by Supplier to meet a Service Level, as well as any failures that subsequently occur as a direct, logical and unavoidable part of the original failure.

8.8 Excused Performance

In addition to the dependencies set forth in Section 8.8 above, Supplier shall not be liable for any failure to meet or exceed the Service Levels, and such failure will not be used for establishing any termination event, to the extent such failure was caused by one or more of the following: (i) a failure of Customer or any of its employees, agents or contractors (including Third Party Providers) to perform any of its responsibilities under the Master Agreement; (ii) any act or omission of Customer or any of its employees, agents or contractors (including Third Party Providers or other third parties acting on behalf of Customer); (iii) reductions in resources designated to the performance of Services requested or approved by Customer; (iv) any hardware, software or other product of a third-party; (v) any failure of Customer to secure the proper access rights or maintenance and support services with respect to any component of the Services (e.g., hardware, software, network, maintenance) for which Supplier does not bear operational responsibility; (vi) downtimes resulting from agreed-upon maintenance windows; or (vii) Customer's reprioritization of the tasks to be performed by Supplier where such reprioritization causes Supplier to miss a Service Level; (viii) declared disasters; or (ix) Adjustment Events.

8.9 Changes to Service Levels

The Parties may agree to modifications to Service Levels through a change order.

8.10 Service Level Credit

Customer shall be entitled to recover a Service Level Credit of up to a maximum of five percent (5%) of Capgemini's total Monthly Base Fees for the applicable month for all Services. Service Level Credits during a period are cumulative; provided, however, the maximum cumulative Service Level Credit to which Customer shall be entitled in a single month is equal to five percent (5%) of Capgemini's Monthly Base Fees for the applicable month (excluding pass-through expenses and special charges, if any). Service Level Credits shall be calculated as follows for each Service Level failure:

Service Level Credit = A x B x C

A= The Monthly Base Fees multiplied by

B= The Service Level Credit (5%) multiplied by

C= Weighting Percentage for the Service Level (per table in Section 8.4)

Where a singled incident results in more than one Service Level Failure, it shall count as only one Service Level Failure for the month in question. For clarification, the Parties expressly acknowledge that the Service Level Credit(s) shall not apply to charges, if any, for expenses, Customer pass-through expenses, special charges, or taxes.

Capgemini may earn back a Service Level Credit if Capgemini's performance of the Service Level for which Customer earned the Service Level Credit meets the Service Level requirements for the three (3) consecutive months immediately following such Service Level Failure (an "Earnback"). Capgemini will be entitled to recover the Earnback by adding an amount equal to the Service Level Credit to the invoice for the month immediately following the month in which Capgemini became entitled to the Earnback. If Capgemini achieves an Earnback for which a Service Level Credit has been previously invoiced, Capgemini will charge Customer the amount of the Earnback on the next invoice following the achievement of such Earnback.

9. ADDITIONAL TERMS

9.1 Changes to Services

- (i) The Parties agree that from time to time during the Term of this SOW, Customer may request, or Supplier may propose, that Supplier implement a change to the Services that may require an extension in the schedule, an adjustment in the fees and expenses and/or an adjustment in the work Supplier is to perform under this SOW, including a change to the scope or the

functionality of the Services or Deliverables (each, a **“Change”**).

- (ii) The Parties also acknowledge and agree that the occurrence of one or more of the following events (each, an **“Adjustment Event”**) may require an extension in the schedule, an adjustment in the fees and expenses and/or an adjustment in the work Supplier is to perform under this SOW: (a) a material change to or deficiency in the information which Customer has supplied to Supplier (including with respect to any Customer Data); (b) a failure by Customer and/or Third Party Providers to perform any of their respective responsibilities, or to provide adequate resources or information, in a timely manner; (c) an unanticipated event that materially changes the Service needs or requirements of Customer; (d) Force Majeure Events; or (e) a change in Law.
- (iii) In the event that an Adjustment Event occurs, or the Parties agree on a Change, Supplier may prepare and provide to Customer a proposed change order identifying the impact and setting forth any applicable adjustments in the Services, Deliverables, schedule and/or fees and expenses. In the event that the Parties' respective authorized representatives reach agreement as to the proposed change order, each Party shall execute the change order and the agreed upon adjustments shall constitute Services. If they are unable to reach an agreement, they shall refer that matter to the Parties' respective senior executives who will negotiate in good faith in an attempt to reach an agreement. If the Parties fail to reach agreement, Supplier shall not be obligated to perform any additional or modified Services and either Party shall be free to pursue alternative remedies.
- (iv) Notwithstanding the foregoing, if any delays or deficiencies in the Services or Deliverables occur as a result of Adjustment Events or Changes, the scheduled completion date for the affected Services and/or Deliverables under this SOW shall be extended to the extent of any such delays, and Supplier shall not incur any liability as a result of such delays or deficiencies. Supplier will use reasonable efforts to perform notwithstanding the Change or Adjustment Event, but Customer will reimburse Supplier for any and all additional fees and expenses incurred by Supplier as a result of any delays or deficiencies resulting therefrom.

9.2 New Services

- (i) New Services. Customer will notify Supplier of any services that Customer desires to receive that are materially different in type from the Services that Supplier is providing pursuant to this SOW (**“New Services”**). Customer shall describe the New Services in reasonable detail in writing to Supplier.

9.3 Required Consents

On or before the Effective Date, Customer, at its cost and expense, represents and warrants that it has obtained and provided to Supplier all consents or approvals required for the right to use, access, and if necessary, modify, applicable third party agreements and the products and other items (including software, equipment and other hardware) which Supplier may need in the provision of Services (**“Required Consents”**), including the consent of third parties for Supplier to relocate their software and equipment in the event that Supplier rearranges or relocates the facilities it uses to provide the Services. Supplier will reasonably assist Customer in obtaining the Required Consents. If any Required Consent is not obtained for any third party agreement, unless and until such Required Consent is obtained, the Parties will cooperate with each other in achieving: (i) a reasonable alternative arrangement for Supplier to provide the Services; or (ii) a revised scope of Services with minimum interference to Customer's business operations, without violation of any third party obligations of either party. If such alternative arrangement is required for a sustained period, the Parties will equitably adjust the affected terms and prices specified in this SOW (including, without limitation, the Service Levels) to permit the Parties to realize the intended benefits and results of this SOW.

9.4 Resource Responsibility

Customer will retain responsibility for the equipment and third-party software, including software upgrades, development tools and workstations, voice and data communications costs, and data center and network infrastructure relating to the Services, except as indicated as a Supplier responsibility in this SOW and for any Supplier provided tools if so provided and used in performance of the Services.

9.5 Customer Third Party Providers

- (i) Customer shall not have the right to engage a third-party provider to perform any services within the scope of the Services (a **"Third Party Service Provider"**) without the prior written consent of Supplier. Customer shall be entitled to engage third-party providers to provide operational support services to Customer that are related to, but not within the scope of, the Services (a **"Third Party Support Provider"**) without Supplier's consent. For the purposes of this SOW, Third Party Service Providers and Third-Party Support Providers are referred to individually as a **"Third Party Provider"** and collectively as **"Third Party Providers"**.
- (ii) If Customer engages a Third Party Provider, such Third Party Provider will be required to enter into an agreement with Customer which establishes performance standards, including any applicable service levels, as necessary to ensure that Supplier will be able to perform the Services in accordance with the performance standards applicable to this SOW (an **"Operating Agreement"**). In addition, Customer will cause each Third-Party Provider to comply with Supplier's security and confidentiality requirements, standards, methodologies and procedures, as applicable. Supplier may, but shall not be obligated to, assist Customer in (a) the negotiation of the terms and conditions for the engagement of such Third Party Provider, and (b) the management or administration of the performance of such Third Party Provider, including with respect to all applicable performance standards required to enable Supplier to meet its corresponding obligations under this SOW. Supplier's obligation to perform in accordance with the performance standards set forth herein is contingent on the Third-Party Provider's performance of its obligations in accordance with the applicable Operating Agreement and any other applicable Third Party Provider performance standards, including any applicable service levels.
- (iii) Supplier will not be responsible or liable for the acts or omissions of a Third Party Provider, and Customer will pay Supplier at its then-current time and materials rates and reimburse Supplier for any expenses incurred for any additional work by Supplier attributable to Supplier's cooperation with the Third Party Provider, integration of the Third Party Provider's services with Supplier's Services, or the performance of Services as a result of any acts or omissions of the Third Party Provider; and all performance standards (e.g., termination rights, remedies, etc.) will be suspended with respect to any software, Services, Deliverables, hardware or systems that have been affected by the Third Party Provider.

9.6 Changes in Law

Customer shall be responsible for compliance with and notify Supplier of any change in law and the adoption of any new law applicable to the businesses in which Customer and Services recipients engage and that are addressed in this SOW or otherwise applicable to the business Customer and Services recipient may from time-to-time conduct, which may affect and/or otherwise influence the Services provided by Supplier.

9.7 Contract Expiration and Transition Services

If requested in writing by Customer, Supplier shall provide reasonable transition assistance to Customer upon expiration of this SOW as are agreed to by the Parties in writing. These services will be billed at Supplier's standard rates and are contingent upon Customer being current in its payments. No Service Levels shall apply to such services.

9.8 Intellectual Property Rights

For purposes of this SOW only, the following provisions shall apply notwithstanding anything to the contrary in the Master Agreement. Nothing contained in this SOW will require either Party to violate the proprietary rights of any third party in any software or other intellectual property.

9.8.1 Customer Data

Information relating to Customer that is contained in Customer's data files (**"Customer Data"**) is the exclusive property of Customer. Supplier is authorized to have access to and make use of Customer Data as appropriate for the performance by Supplier of its obligations under this SOW. Upon the termination or

expiration of this SOW, Supplier will use commercially reasonable efforts to return to Customer or destroy all Customer Data in Supplier's then-existing machine-readable format and media in accordance with Customer's instructions and at Customer's expense. Supplier will not use Customer Data for any purpose other than providing the Services or Deliverables.

9.8.2 Customer Software

Except as otherwise provided in this SOW, software owned by Customer will remain Customer's property and Supplier will have no ownership or other rights or interests in Customer software. Customer hereby grants to Supplier (and to the other Supplier Entities to the extent necessary for Supplier to perform the Services) a non-exclusive, perpetual, worldwide, paid-up right and license to access, use, operate, reproduce, display, perform, modify, enhance, distribute and create derivative works of any of the Customer software which is necessary or desirable to perform the Services, without charge to Supplier. Customer will make the Customer software available to Supplier in such form and on such media as Supplier may reasonably request, together with existing documentation and other materials.

9.8.3 Supplier Software

All Supplier software, including all the same that constitute technical elements, will remain Supplier's property and Customer will have no ownership or other rights or interests therein.

Except as otherwise expressly provided in this SOW, during the Term, Customer will pay all required license, installation, maintenance and upgrade fees with respect to any third-party software that Customer licenses ("**Customer- Supplier Software**"), or that Supplier licenses solely for its use in providing the Services ("**Dedicated Supplier Software**"). Customer will obtain all Required Consents necessary to permit Supplier to access or operate the Customer-Supplier Software and Dedicated Supplier Software and to directly contact the vendors to obtain support for such software, and Customer will pay all costs and expenses associated therewith. Customer will provide written evidence of such Required Consents to Supplier upon Supplier's request. Customer- Supplier Software will be made available to Supplier on or before the Effective Date in such form and on such media as Supplier may reasonably request, together with appropriate documentation and other materials.

To the extent expressly set forth in this SOW, Supplier will obtain all consents necessary to permit Supplier to access or operate any software that Supplier licenses from third parties and uses to provide Services to Customer and to other customers on a shared basis ("**Shared Supplier Software**"). During the Term, Supplier will pay all required license, installation, maintenance and upgrade fees with respect to the Shared Supplier Software.

9.9 Relocation of Services

Notwithstanding anything to the contrary in the Master Agreement, upon Customer's consent, which consent shall not be withheld unreasonably, Supplier may rearrange and relocate the Services, equipment, or software as Supplier deems necessary in order to perform the Services in accordance with this SOW.

9.10 Advancements in Technology

Notwithstanding anything to the contrary in the Agreement, Supplier may, in its sole discretion and at its expense, implement technological advancements relative to the provision of the Services so long as Supplier continues to perform the Services in accordance with the Service Levels set forth in this SOW.

9.11 Cooperation

- (i) Customer will establish, in coordination and cooperation with Supplier, appropriate priorities for the Services and communicate such priorities to Supplier, including the confirmation and prioritization of requests for maintenance, enhancements, and new application development.
- (ii) Customer will cooperate with and assist Supplier by making available, as reasonably requested by Supplier, management decisions, information, approvals, acceptances, and access to key decision makers, managerial, administrative and technical personnel, in order that the obligations of Supplier under this SOW may be properly and timely performed.
- (iii) Customer will provide Supplier with all data and information in suitable electronic format, as may be necessary or appropriate to enable Supplier to perform the Services in a timely manner and Customer shall otherwise fully cooperate with Supplier in connection therewith. Customer

will be responsible for the accuracy and completeness of Customer Data.

9.12 Review of Deliverables

Each of the Deliverables, reports and other output prepared by Supplier shall be timely reviewed and approved or rejected by Customer in accordance with the criteria, timing and procedures set forth in this SOW or as otherwise mutually agreed in writing by the Parties.

9.13 Retained and Pass-Through Expenses

Except as set forth below, the amounts charged by Supplier will not include various expenses that will be retained by Customer or passed through to Customer with an administrative charge. Customer will pay directly to the applicable vendors the expenses that are to be retained by Customer ("**Retained Expenses**") associated with the Services, and the expenses that are incurred by Supplier as part of providing the Services but are to be passed through to Customer ("**Pass-through Expenses**"), both as specified in this SOW. Where applicable, Supplier will provide Customer with information necessary to permit Customer to pay Pass-through Expenses, and Customer will provide Supplier written confirmation of payment. In the event that Customer does not pay Pass-through Expenses, Supplier has the right to make such payments and Customer will reimburse Supplier for those payments. Customer will hold Supplier harmless for any payments made by Supplier pursuant to this paragraph. If Supplier implements cost savings measures that result in a reduction of Pass-through Expenses, Customer shall pay to Supplier a bonus equal to the actual aggregate amount of such reduction during the first twelve (12) Months after such measures first go into effect. Supplier will not reduce any Pass-through Expenses in a manner that would entail a reduction of the Service Levels associated with such expenses without Customer's approval. Supplier may receive credits or payments for purchases from third party vendors, which shall not alter or reduce Customer's obligation to pay expenses as invoiced by Supplier and referenced herein.

9.14 Supplier Warranties

Supplier does not warrant or have liability for the services of a common carrier (e.g., Federal Express, UPS, or postal service) or warehouseman (e.g., Iron Mountain), if applicable. Where Supplier procures hardware, software, and/or maintenance services on Customer's behalf, such items are not warranted by Supplier, and Customer waives any claim against Supplier for the performance or quality of these items or warranties on the items; provided that the foregoing does not affect Supplier's specific Service performance responsibilities as otherwise set forth in this SOW. To the extent that the vendor has made any warranties to Supplier that Supplier has the right to assign to Customer, Supplier agrees to assign to Customer such warranties. In addition, Supplier shall use its commercially reasonable efforts to enforce, on Customer's behalf, at Customer's sole additional expense, any other warranties that the vendor has made to Supplier with respect to the items. Customer acknowledges that Customer is not relying on any representations made by Supplier with respect to the items.

9.15 COVID

Customer acknowledges that any delay in Supplier's performance or inability of Supplier to perform hereunder due to conditions or circumstances related to COVID-19, regardless of foreseeability, will relieve Supplier of its performance obligations hereunder. In such event, Supplier will provide notice to Customer of known impacts and use commercially reasonable efforts to mitigate any Services disruption. The parties will work in good faith to reach a mutual agreement regarding changes to the approach, schedule, or other aspect of the Services that may be necessary. Without limiting the foregoing, Customer acknowledges that Supplier personnel will work from their home locations to perform Services under this SOW and Customer acknowledges that any requirement for onsite performance (whether at Customer or Supplier offices), and any corresponding contractual obligations relating to onsite performance, shall not apply.

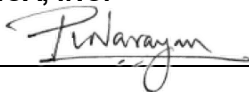
9.16 Miscellaneous

Customer is solely responsible for determining its requirements and specifications to address its legal or regulatory compliance, including its Sarbanes-Oxley compliance. Supplier is not providing any legal advice to the Customer and does not warrant that any Services it provides will assist Customer in being compliant with its legal or regulatory compliance. To the extent applicable to any of the Services, Customer will consult with and rely exclusively on its own legal counsel for legal advice.

IN WITNESS WHEREOF, Capgemini and MoneyGram have caused this Statement of Work to be executed by their respective duly authorized representatives effective as of the Effective Date.

CAPGEMINI AMERICA, INC.

By: _____

Printed Name: Narayan PuthanmadhomTitle: EVP

August 28, 2023

MONEYGRAM PAYMENT SYSTEMS, INC.

By: _____

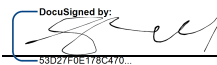
Printed Name: Anna GreenwaldTitle: Chief operating officer

EXHIBIT A-3



Cory J. Feinberg, Esq.
General Counsel,
Corporate Secretary

October 3, 2024

Capgemini America, Inc.
79 Fifth Avenue, 3rd Floor
New York, NY 10003
Attention: General Counsel

As you have previously been made aware, MoneyGram has launched a full-scale investigation regarding the cybersecurity incident that occurred on September 20, 2024 (the "Incident"). As the Incident arose from social engineering through Capgemini's Service Desk Managed Services, Capgemini is bound to "maintain and preserve all documents, records and other data related to the Incident" under Section 7.3 of the Data Processing and Data Security Addendum ("Data Security Addendum") to the Business Services Master Agreement (the "MSA"). In connection with our ongoing investigation, MoneyGram instructs Capgemini to fully comply with Section 7.3 and preserve all such documents, including but not limited to:

- 1) All recordings and/or transcripts of MoneyGram-related calls to and from the IT Help Desk on September 19 and 20, 2024, as well as MoneyGram-related calls for the 6 months prior to September 20, 2024;
- 2) All records, policies and procedures relating to Capgemini's implementation and operation of any systems used to comply with the Data Security Addendum;
- 3) All Background checks, as described in Section 1.6 of the MSA, for any personnel providing services to MoneyGram;
- 4) All policies, procedures, training materials or other documents pertaining to the personnel providing services to MoneyGram.
- 5) All certificates of insurance, as described in Section 6 of the MSA;
- 6) All documents describing the Security Breach Procedures described in Section 7 of the Data Security Addendum;
- 7) All documents, including emails, texts, messages and/or reports, relating to the Incident; and.
- 8) All relevant records, logs, files, data reporting and other materials relating to the Incident.



MoneyGram is working with numerous third parties and regulators in connection with this investigation and expects Capgemini to fully comply with its obligation to assist MoneyGram with its investigation, provide MoneyGram with physical access to the facilities and operations affected, facilitate interviews with the persons involved in the Incident and to make available all relevant materials, each as more fully described in Section 7.2 of the Data Security Addendum. To that end, MoneyGram requests that Capgemini immediately provide the documents requested above no later than October 11, 2024.

Please acknowledge receipt of this request and Capgemini's willingness to fully comply with its obligations under the MSA, its addendums and Statements of Work.

Sincerely,

A handwritten signature in blue ink, appearing to read 'Cory J. Feinberg'.

Cory J. Feinberg
General Counsel
MoneyGram International, Inc.

EXHIBIT A-4



Capgemini America, Inc.
Office of General Counsel

October 31, 2024

Via E-Mail: cfeinberg@moneygram.com

Cory J. Feinberg, Esq.
General Counsel
MoneyGram
2828 N. Harwood Street – 15th Floor
Dallas, TX 75201

RE: *MoneyGram document production demand*

Dear Mr. Feinberg:

Capgemini America, Inc. (“Capgemini”) is in receipt of your letter dated October 3, 2024, requesting that Capgemini preserve and produce documents and information regarding a cybersecurity incident occurring on September 20, 2024.

In response to the production request, Capgemini provides the following documents, redacted as appropriate:

- Log identifying all MoneyGram related calls to and from the IT Help Desk on September 19 and 20, 2024;
- 9/20/24 email to Marco Mannetta providing notice of the suspected phishing calls, with attached 4 call recordings;
- 9/30/24 email to Marco Mannetta providing 2 additional call recordings upon Marco’s request;
- 10/4/24 email to Marco Mannetta providing 3 more call recordings upon Marco’s request;
- 4/8/24 email to Marco Mannetta regarding requested knowledge base article “KB0033815: Active Directory(AD)/LAN Password reset process”;
- 9/26/24 email providing How To instructions “Clear Local AppData from VDI User Profile.

It is our understanding that MoneyGram has already been provided copies of the 4 call recordings in question, on the date of original notification on September 20, 2024, as well as 5 other call recordings upon Marco’s request. Additionally, copies of the applicable Certificates of Insurance were provided on October 28, 2024. Further, we have been advised that all other records, policies, procedures and training materials regarding the Help Desk functions performed by our employees for MoneyGram, are all maintained exclusively on the MoneyGram platforms, including Service Now, to which our employees no longer have access.

If you have any questions or concerns, please do not hesitate to contact me at Traci.Zalinski@capgemini.com.

Sincerely,

Capgemini America, Inc.

Traci Zalinski

Associate General Counsel
Litigation & Employment and Ethics Officer

EXHIBIT A-5

O'Melveny & Myers LLP
2801 North Harwood Street
Suite 1600
Dallas, TX 75201-2692

T: +1 972 360 1900
F: +1 972 360 1901
omm.com

File Number:

November 27, 2024

Scott Drake
D: +1 972 360 1915
sdrake@omm.com

Attention: General Counsel
Capgemini America, Inc.
79 Fifth Avenue, 3rd Floor
New York, NY 10003

Re: Cybersecurity Incident that occurred on September 20, 2024

Dear Counsel:

We have been retained by MoneyGram International, Inc. ("MoneyGram") in connection with the cybersecurity incident that occurred on September 20, 2024 (the "Incident"). Pursuant to Section 8.2 of the Business Services Master Agreement (the "MSA") and Section 9 of the Data Processing and Data Security Addendum, Exhibit D to the MSA, ("Data Security Addendum"), MoneyGram provides notice to Capgemini America, Inc. ("Capgemini") of the following lawsuits filed against MoneyGram arising out of a breach of the Data Security Addendum resulting from the negligent acts or omissions of Capgemini. Per the MSA, MoneyGram is entitled to indemnity from Capgemini for all losses, costs, expenses (including reasonable attorney fees) and other "Losses" as more fully described in the MSA. To date, MoneyGram has been named in the following lawsuits, for which MoneyGram demands indemnity:

Larion Krayzman v. MoneyGram Payment Systems, inc.	US District Court, Central District of California	2:2024-cv-09513-AB-JPR
Letia Dickerson v. MoneyGram Payment Systems, Inc. and MoneyGram International, Inc.	US District Court, Northern District of Texas	3:2024-cv-02604-B
Carnel Faulkner v. MoneyGram Payment Systems, Inc. and MoneyGram International, Inc.	US District Court, Northern District of Texas	3:2024-cv-02557-S
Mosima Namata v. Moneygram Payment Systems, Inc.	US District Court, Northern District of Texas	3:2024-cv-02571-X
Armando Reyes v. Moneygram Payment Systems, Inc.	US District Court, Northern District of Texas	3:2024-cv-02572-N

Roy Uribe v. MoneyGram Payment Systems, Inc.	US District Court, Northern District of Texas	3:2024-cv-02573-L
Steven Drake v. MoneyGram Payment Systems, Inc.	US District Court, Northern District of Texas	3:2024-cv-02647-X
Mosanthony Wilson v. MoneyGram Payment Systems, Inc.	US District Court, Northern District of Texas	3:2024-cv-02772-E
Humayun Mahmood v. MoneyGram Payment Systems, Inc. and MoneyGram Payment Systems Canada, Inc.	Supreme Court of British Columbia, Canada	VLC-S-S-247342

This notice is without waiver of any of MoneyGram's rights to seek further indemnity and/or damages resulting from the Data Incident. MoneyGram is still incurring damages caused by Capgemini's role in the Data Incident. MoneyGram intends to make further claims for indemnity and recovery of significant damages in the near future.

Sincerely,



Scott Drake